

Channel capacity of polar coding with a given polar mismatched successive cancellation decoder

Mine Alsan

Department of Electrical and Computer Engineering

National University of Singapore, Singapore

Email: minealsan@gmail.com

Abstract

Arkan's polar coding, is by now a well studied technique that allows achieving the symmetric capacity of binary input memoryless channels with low complexity encoding and decoding, provided that the polar decoding architecture is used and the decoding metric is matched to the true channel. In this paper, we analyze communication rates that are achievable when the polar coding/decoding architecture is used with the decoder using an incorrect model of the channel. We define the 'polar mismatched capacity' as an analogue of the classical mismatched capacity, give an expression for it, and derive bounds on it.

Index Terms

Channel polarization; polar codes; mismatched successive cancellation decoders; mismatched polar decoders; polar mismatched capacity; mismatched decoding; mismatched capacity

I. INTRODUCTION

In various communication scenarios, we encounter sub-optimal decoders due to partial or missing channel information or practical implementation constraints. To give an example of an obstacle on the way of optimal decoding, we can consider the case where a high signal

The material in this paper was presented in part at the IEEE Information Theory Workshop, Sevilla, Spain, 2013, and at the IEEE Information Theory Workshop, Hobart, Australia, November 2014.

to noise ratio channel is used with a large constellation with points indexed by k -bit symbols $s(0\dots 0), \dots, s(1\dots 1)$, and the receiver is interested in recovering the 1st of these k bits. Then, the true likelihood ratio requires the computation of the sums

$$\sum_{b_2, \dots, b_k} W(y|s(0, b_2, \dots, b_k)) \quad \text{and} \quad \sum_{b_2, \dots, b_k} W(y|s(1, b_2, \dots, b_k)),$$

each containing an exponential number of terms (in k). The receiver hardware may not permit such computations, and the decoder designer may be forced to use a simpler metric $V(y|1)/V(y|0)$ which approximates the true one. In such cases, even when the receiver is informed of the true channel W , the decoding operation proceeds on the basis of a mismatched channel V . Regardless of the nature of the obstacle, sub-optimal decoders might perform worse than optimal decoders minimizing the average decoding error probability and result in capacity loss. Modeling such sub-optimal scenarios via ‘*reliable communication with a given decision rule*’ and establishing coding theorems for them allows one to assess the extent of any loss.

Due to their many desirable properties, among which good performance and low complexity, polar codes are being considered as candidate error correction codes for use in future wireless communication systems. The ideas behind polar coding, which we will discuss later in details, make successive cancellation decoding of polar codes the choice of decision rule for developing an elegant yet practical theory. Although successive cancellation decoding is a sub-optimal decision procedure, most of the results developed so far, and in particular those of theoretical nature, including the initial theory in [1] and multiple extensions to it, make the assumption that the polar coding scheme is used with a specific successive cancellation decoder architecture in which the decoding metric is matched to the true channel. The analysis provided in [1] shows that it is possible to achieve the symmetric capacity of binary input discrete memoryless channels (B-DMCs) using the polar coding scheme, and thus, the use of a successive cancellation decoder does not result in any capacity loss.

On the other hand, as we have just discussed, it may not be possible for the implemented decoder to make its computations based on a decoding metric that is exactly matched to the true channel due to complexity or feasibility requirements. Such limitations, in turn, bear important engineering implications for system designers: Take for instance the work in [2] which investigates the problem of optimally assigning a mismatched metric to the received signal from a constrained finite set of metrics, driven by the consideration that, in practice, the receiver implementation will not permit infinite-precision arithmetic. Motivated by these observations, the

primary objective of this paper is to study the effects of a decoding mismatch on the transmission capacity of polar coding over B-DMCs.

A. Preliminary Notations

Let $W : \mathcal{X} \rightarrow \mathcal{Y}$ denote a discrete memoryless channel (DMC) with input alphabet \mathcal{X} , output alphabet \mathcal{Y} , and transition probabilities $W(y|x)$, for $x \in \mathcal{X}$ and $y \in \mathcal{Y}$. When W is a B-DMC, we will use the notation $\mathbb{F}_2 := \{0, 1\}$ to denote the input alphabet of the channel. When the distribution of the channel input random variable X is $P(X)$, this is denoted as $X \sim P(x)$. In this case, the distribution of the channel output random variable Y is given by

$$PW(y) = \sum_{x \in \mathcal{X}} P(x)W(y|x), \quad (1)$$

and we have $Y \sim PW(y)$.

For a given DMC $W : \mathcal{X} \rightarrow \mathcal{Y}$, we further define

$$W(\{y : y \in \mathcal{S}\}|u) := \sum_{y \in \mathcal{S}} W(y|u), \quad (2)$$

for $u \in \mathcal{X}$ and $\mathcal{S} \subseteq \mathcal{Y}$. Similarly, if we have a random variable Q defined on a probability space $(\Omega, \mathcal{F}, \mathbb{P})$, we define

$$\mathbb{P}(\{\omega : Q(\omega) = q\}) := \sum_{\omega \in \Omega} \mathbb{P}(\omega) \mathbf{1}\{Q(\omega) = q\}, \quad (3)$$

As customary, the expectation operator for random variables is denoted by $\mathbb{E}[\cdot]$.

The notation $\mathcal{A}_N \subseteq \{1, \dots, N\}$ is used, and the complement of this set is denoted by $\mathcal{A}_N^c = \{1, \dots, N\} \setminus \mathcal{A}_N$. The notation \log stands for the base 2 logarithm, and \ln stands for the natural logarithm. The notation $|x|^+ = \max\{x, 0\}$ is used. As usual, the set of non-negative integers is denoted by \mathbb{N} . Finally, standard Landau notations $O(\cdot)$, $o(\cdot)$, and $\omega(\cdot)$ are used throughout the paper to denote the asymptotic behavior of functions.

B. Paper Outline

The rest of the paper is organized as follows. Section II briefly surveys the literature on the subject of reliable communication with a given decision rule. Section III introduces the main concepts of polar coding and the definition of the mismatched polar decoder. Then, an overview of the main results of this paper is presented in Section IV, where the main theorems are stated through Theorems 5–9, and the results proved in Section V. Finally, the paper concludes with some final remarks given in Section VI.

II. RELIABLE COMMUNICATION WITH A GIVEN DECISION RULE

One of the main subjects that sparked the development of the field of information theory is the problem of reliable communication over a single point-to-point channel. Shannon formulated a theoretical framework to address this engineering problem by introducing a mathematical model of a communication system, and considering how one can measure in such a model the capacity of a channel to transmit information [3]. Formal definitions introduced since then became well-established.

An (M, N, ϵ) block code for a DMC $W : \mathcal{X} \rightarrow \mathcal{Y}$ is an N -length block code characterized by (i) a sequence of M codewords $\mathbf{x}(i) \in \mathcal{X}^N$, for $i = 1, \dots, M$, (ii) a sequence of disjoint decoding regions $\mathcal{B}_i \subseteq \mathcal{Y}^N$ for each codeword $\mathbf{x}(i)$, and (iii) a maximum or average error probability that is at most ϵ , with $\epsilon > 0$. A number $R \geq 0$ is an achievable transmission rate for the DMC W , if there exists a sequence of $(2^{NR}, N, \epsilon_N)$ codes such that $\epsilon_N \rightarrow 0$ as $N \rightarrow \infty$. In other words, a coding scheme is designed so that the channel encoder can map each message to a codeword by adding redundant information, such that upon reception, the corresponding channel decoder can overcome the effects of noise introduced during transmission and decode the messages with an arbitrarily small probability of error when the block-length is sufficiently large.

The channel capacity of a DMC $W : \mathcal{X} \rightarrow \mathcal{Y}$ corresponds to the highest achievable rate $T(W)$ that information can be sent through the channel. Its operational meaning imposes a limitation on the maximum number of possible messages, and hence codewords, that can be conveyed through the system. Shannon [3] showed that this rate is given by the quantity $C(W) = \max_{P(x)} I(P, W)$, where the maximization is over all possible channel input distributions $P(x)$, for $x \in \mathcal{X}$, and the mutual information between the channel input $X \sim P(x)$ and output $Y \sim PW(y)$ is given by

$$I(P, W) = \sum_{x \in \mathcal{X}} \sum_{y \in \mathcal{Y}} P(x) W(y|x) \log \left(\frac{W(y|x)}{PW(y)} \right). \quad (4)$$

The proof of this result breaks into two parts. The “converse” part consists of showing that $T(W) \leq C(W)$ holds by proving a statement of the following form: Given $R > 0$, any code for W having rate $R > C(W)$ cannot have $\epsilon_N \rightarrow 0$ as $N \rightarrow \infty$. The statement follows from Fano’s and data processing inequalities, see for instance [4], and the derivation does not depend on any particular type of encoding and decoding procedures which might be employed by the system. The “direct” part, on the contrary, shows that $T(W) \geq C(W)$ is achievable by demonstrating that

for a given $R > 0$, there *exists* a sequence of $(2^{NR}, N, \epsilon_N)$ codes for W having rate $R \leq C(W)$, and such that $\epsilon_N \rightarrow 0$ as $N \rightarrow \infty$.

Shannon's analysis [3] reveals that it is possible to prove a channel coding theorem showing the existence of codes achieving the channel capacity without even the need to explicitly construct one such code. This approach, known as the random coding argument, involves specifying an encoding procedure to generate a random code from an ensemble of codes and a decoding procedure so as to measure the error probability averaged over the code ensemble. Note that since the decoder declares that the codeword $\mathbf{x}(i)$, for $i = 1, \dots, M$, is sent if and only if the received output sequence $\mathbf{y} \in \mathcal{B}_i$, and otherwise declares an error, in order to work on the decoding error probability, the decoder must be given a decision rule to emulate the partitioning of the output space into decoding regions. The random coding argument used in [3] involves an ensemble of randomly generated i.i.d codes and a typicality decoder.

An alternative random coding argument for the direct part is provided by Gallager's refined error analysis. The noisy channel coding theorem [4, Chapter 5] states that for a given DMC and a fixed rate $R > 0$, the average maximum likelihood (ML) decoding error probability of an ensemble of block codes of block-length N is upper bounded by $4 \exp\{-NE_r(R)\}$. The exponent $E_r(R)$, denoting to the random coding exponent of the ML decoder, takes positive values only for fixed values $R < C(W)$. The established speed of convergence of the error probability to zero, which is in this case exponential, uncovers a trade-off between critical design parameters of a communication system. A slight variation of the union bound is used to compute an upper bound to the union of all the events which cause the decoder to make an error.

Yet another proof of the direct part is given by Csiszár et. al [5], see also [6], by relying on constant composition codes and a decoder known as the maximum mutual information (MMI) decoder. Introduced by Goppa [7], this is a decoder which declares an input message if and only if the corresponding codeword maximizes the empirical mutual information computed from the joint empirical distribution of the codeword and the received channel output sequence. To proceed with the performance analysis, the method of types [8] is used as a tool to analyze sequences partitioned into classes according to their types (empirical distributions). For instance, the set of output sequences is partitioned into conditional type classes for given codewords to begin the analysis. An exponential upper bound on the error probability is obtained by summing the probabilities of the union of the error events and then by exercising the theory of types on this sum. The random coding exponent of the MMI decoder for a constant composition code of type

\hat{P} is positive if and only if $R < I(\hat{P}; W)$ [8, Theorem IV.1].

Furthermore, since the MMI decoder does not depend on the channel, the method of types produces a coding theorem which also applies to situations where the law of the DMC is unknown to the code designer. It follows from [8, Theorem IV.1] that universally attainable transmission rates can be obtained over any DMC without the knowledge of the true channel. Thus, the problem of reliable point-to-point communication over DMCs without channel information is solved with the help of a universal decoder which does not depend on the channel. However, even though the MMI decoder is more robust than typicality and ML decoders which require the exact channel knowledge to function, they all come short in practice due to their highly complex computational natures.

In the discussed treatments of the direct part, the main concern of the authors was to theoretically explore the achievability criteria over DMCs without imposing constraints on the available resources to encoders and decoders or expecting compliance with various requirements real applications might have. While significant insights have been gained, new tools have emerged, and the proof techniques have been applied in many other contexts, no practical capacity-achieving coding scheme has originated from these studies. Progress in that area got sought in parallel along other lines of research, and the field of coding theory has started to expand with the aim of bridging the gap of theory with practice by finding *provably* capacity achieving codes that are also amenable to practice. A historical account on the evolution of channel coding can be found in the survey article [9]. Ultimately, Arıkan [1] came up with the polar coding method which provided for the first time a code construction method demonstrated to achieve the channel capacity of B-DMCs with low complexity encoders and decoders. See also [10] for an account on the considerations that motivated the development of polar coding to learn about interesting details that are hidden behind the state-of-the-art polar coding literature .

A. Mismatched decoders

Decoders can be categorized into families based on the type of decision rule they are using. This allows their study within a unified framework. Alpha (α) decoders are one such family accommodating decision rules which are based on the joint empirical distributions of the codewords and the received channel output sequences [8]. For instance, the MMI decoder belongs to the family of α -decoders. Given a set of codewords $\mathbf{x}(i) \in \mathcal{X}^N$, for $i = 1, \dots, M$, and a received sequence $\mathbf{y} \in \mathcal{Y}^N$, an α decoder declares that message $i = 1, \dots, M$ was sent if and only if

$\alpha(\mathbf{x}(i), \mathbf{y}) < \alpha(\mathbf{x}(j), \mathbf{y})$ holds for all $j \neq i$. If there is no such index i the decoder declares an erasure. Using the method of types, Csiszár and Narayan [11] analyzed the performance of this family of decoders over DMCs and derived the random coding exponent of α -decoders used with constant composition codes. See [12, Eq. (6)] for the expression of this exponent.

Since, in general, α -decoders are too complex to be implementable, Csiszár and Narayan [12] studied subsequently the performance of a more restricted family of decoders called d -decoders. A d -decoder is an α -decoder whose decision function can be computed using the additive extension of a single letter metric $d(x, y)$, where $x \in \mathcal{X}$ and $y \in \mathcal{Y}$. The transmission capacity of the channel $W : \mathcal{X} \rightarrow \mathcal{Y}$ when decoded with an additive metric d is denoted by $C_d(W)$. Even though the MMI decoder is no longer treated within this family of decoders with additive decision rules, the authors of [12] note that d -decoders still provide a broad enough framework to allow the study of many important decision rules such as the ML or mismatched ML decoding rules, and of difficult information-theoretical problems such as the Shannon capacity of a graph or the zero-error capacity of a DMC [13].

When the metric d corresponds to the likelihood with respect to a mismatched channel V , the d -decoder is called a *mismatched ML decoder* and $C_d(W)$ is called the *mismatched capacity* of the channel W . In this paper, we denote the mismatched capacity by $C(W, V)$. No closed form single letter expression is known for $C(W, V)$ or $C_d(W)$. Single-letter lower bounds have been derived, but no converse for any of the lower bounds exists, except for some very special cases. The class of binary input binary output channels is such a special case where either $C_d(W) = C(W)$ or $C_d(W) = 0$ hold depending on whether or not the mismatch metric is in ‘harmony’ with the channel behavior [12]. Until recently, another exception was thought to be the class of B-DMCs. Balakirsky [14], [15] claimed a converse and gave a computable expression for $C_d(W)$ when W is a B-DMC. However, a recent result of Scarlett et. al. [16] cast doubt on the veracity of Balakirsky’s converse in general by providing a counter-example where superposition coding is shown numerically to achieve a higher rate than Balakirsky’s converse under mismatched ML decoding.

Independently from the study of α -decoders presented in [11] and before the study of d -decoders presented in [12], Hui derived in [17, Chapter 4] a single-letter expression for a lower bound on $C(W, V)$. This lower bound turned out to coincide with the lower bound on $C(W, V)$ given by the more general exponent derived in [11]. An in depth study of the properties of this lower bound, carried out later in [18], introduced the notation C_{LM} to denote this lower bound.

Dubbed as the “LM rate”, C_{LM} became the generally accepted term in the ensuing literature to refer to the lower bound on $C(W, V)$ given in [11] and [17]. It is shown in [18] that if one insists on using a random coding argument, C_{LM} becomes the highest possible achievable rate for mismatched decoding, i.e., the channel capacity of random coding with a given mismatched decoder.

Improvements over the LM rate have been also studied in the literature. The simplest method to improve the lower bound is discussed in [12]: The idea is to recourse to the product space and to apply the arguments that lead to the derivation of C_{LM} to the super-channels $W^N : \mathcal{X}^N \rightarrow \mathcal{Y}^N$ corresponding to N -length blocks¹. It has been conjecture that as $N \rightarrow \infty$, the family of lower bounds tend to $C(W, V)$. However, this improvement comes with a price since it is in general not possible to compute C_{LM} corresponding to the N -th super-channel when N is large. Another improvement over the lower bound C_{LM} was also obtained by Lapidoth [19] which derived a single letter expression by treating the single-user channel as a multiple-access channel. The author also studied in a different work [20] the performance of nearest neighbor decoding for additive non-Gaussian channels as a special case of the general mismatch capacity problem.

We would like to mention at this point that the early literature on d -decoders or the mismatched capacity problem is broader than the pointed references. For instance, ‘erasures only metrics’, a special case of d -decoding such that $d(x, y) = 0$ if and only if $W(y|x) > 0$, have received particular attention in the d -decoding literature [12]. Multiple works such as [21]–[23], and [24] investigated $C_d(W)$, which is called in this case the zero error capacity with erasures or the zero undetected error capacity, and derived lower bounds on this capacity. For a more detailed survey and more extensive list of references on the earlier developments of the subject, we refer the readers to [12], [18], and [25], and the references therein. We should also note that the subject received considerable attention in recent years through the publication of multiple works treating various aspects of the subject, see for instance [26]–[31]. For these latest developments, we refer the readers to [30] and [32], and the references therein.

We do not further elaborate the topic here because the problem setup we are interested in this paper is different and new. In the classical mismatched capacity problem, one fixes the true channel W and a mismatched channel V used by the ML decoder, and then designs a code

¹To be more precise, the corresponding family of lower bounds on $C_d(W)$, denoted as $C_d^{(N)}(W)$, is given in [12], where $C_d^{(1)}(W) = C_{\text{LM}}$ in the case of mismatched decoding. Moreover, note that Balakirsky’s converse [15] coincides with $C_d^{(1)}(W)$.

with the full knowledge of W and V . The classical mismatched capacity is the highest rate for which a reliable code may be designed. In this paper, we take an analogous viewpoint, assume full knowledge of W and V , but insist on using polar codes and polar decoders as opposed to arbitrary codes and ML decoders, and we study the performance of mismatched polar decoders.

Finally, we note that successive cancellation decoders can be considered as another large decoder family based on successive cancellation decoding procedures. They offer a quite different decoding paradigm than additive decoders. A successive cancellation decoder decodes the received output in multiple stages using a chain of estimators each possibly depending on the previous ones. The estimators $\hat{x}_i \in \mathcal{X}$ can base their decisions on arbitrary single letter metrics of the form $d_i(x, y_1^N \hat{x}_1^{i-1})$, for $i = 1, \dots, N$, where N is the block-length, $y_1^N \in \mathcal{Y}^N$ is the received channel output, and $x \in \mathcal{X}$. The successive cancellation decoder of the polar coding scheme, however, is particularly attractive not only for yielding polar coding theorems proving the “symmetric capacity achievingness” of the scheme, but also for its low complexity architecture [1], [33]–[35].

III. POLAR CODING

In his seminal work [1], Arikan introduced polar coding as a method to construct a family of error correcting codes achieving the symmetric capacity of B-DMCs by taking advantage of a phenomenon called channel polarization. Originally, it was shown in [1] that this family of error correcting codes, named as polar codes, features many desirable properties such as being defined with an explicit construction and requiring low complexity encoders and decoders. Subsequently, the polar coding method has been extended to multiple other contexts and it was shown that polar codes achieve the capacity of a large class of channels: the method was extended over larger input alphabet sizes and multiple access channels [36]–[40]; studied in the context of additive white Gaussian noise channels [41], [42]; extended to channels with memory [36]; extended to relay channels [43]; extended to broadcast channels [44]–[46]; extended to quantum channels [47], [48]; extended to non-stationary memoryless channels [49]; extended to fading channels [50]; investigated for energy-harvesting channels [51]; explored for polar coded-modulation [52]; explored in the context of secrecy [53]–[57]; proposed for flash memories [58]–[60]; explored in the design of rateless/rate-compatible family of codes [61], [62]. Furthermore, the polarization phenomenon has been also explored in the context of source coding: the first study on the subject showed that polar codes achieve Shannon’s rate-distortion bound for a large class of sources [63];

later the term ‘source polarization’ was coined by Arkan who applied his technique for lossless source compression [64] and for the Slepian-Wolf problem [65]; and further extensions were studied [66], [67]. A comprehensive survey of all the polar coding literature is beyond the scope of this work, and many other works investigating other important aspects of polar coding have not been cited here. Other than few exceptions, the references included here are mainly limited to transaction level publications and dissertations.

In this section, we review the original polar coding method proposed in [1] for B-DMCs as the same method will play a crucial role in the exposition and understanding of the results in this paper. In addition, we review some of the key aspects of the dominant analysis technique used to prove coding theorems in the context of polar coding. In between, we also present the problem setup by introducing the mismatched polar decoder.

A. Channel Polarization and Polar Codes

Suppose that we are given N independent copies of a B-DMC $W : \mathbb{F}_2 \rightarrow \mathcal{Y}$ with independently and uniformly distributed binary inputs. Let $I(W)$ denote the symmetric capacity of the channel W , which corresponds to the mutual information between the inputs and outputs of the channel evaluated for the uniform input distribution. The polarization effect is observed in [1] by applying a particular channel transformation to the super-channel $W^N : \mathbb{F}_2^N \rightarrow \mathcal{Y}^N$ in order to synthesize another set of N channels that exhibit a certain asymptotic behavior: As N is increased, the synthesized channels polarize into two clusters, having in one group almost perfect channels with symmetric capacities close to 1, and in the other, almost completely noisy channels with symmetric capacities close to 0, for almost all but a vanishing fraction of channels. The particular channel transformation synthesizing the polarized channels is called the channel polarization transformation, and the synthesized channels are denoted by $W_N^{(i)} : \mathbb{F}_2 \rightarrow \mathcal{Y}^N \times \mathbb{F}_2^{(i-1)}$, with indice range $i = 1, \dots, N$. More formally, the channel polarization phenomenon is observed in [1] by proving the following theorem.

Theorem 1. [1, Theorem 1] For any B-DMC W and for all $\gamma \in (0, 1)$,

$$\frac{1}{N} \#\{i \in \{1, \dots, N\} : I(W_N^{(i)}) \in (\gamma, 1 - \gamma)\} \xrightarrow{N \rightarrow \infty} 0, \quad (5)$$

such that

$$\frac{1}{N} \#\{i \in \{1, \dots, N\} : I(W_N^{(i)}) \in (1 - \gamma, 1]\} \xrightarrow{N \rightarrow \infty} I(W), \quad (6)$$

$$\frac{1}{N} \#\{i \in \{1, \dots, N\} : I(W_N^{(i)}) \in [0, \gamma)\} \xrightarrow{N \rightarrow \infty} 1 - I(W), \quad (7)$$

where $N = 2^n$ with $n \in \mathbb{N}$.

From Theorem 1, it can be seen that while the channels $W_N^{(i)}$ get polarized, the fraction of the almost perfect channels tends to the symmetric capacity of the original channel W . This hints that the polarization transformation must be a channel transformation which preserves the average sum of the symmetric capacities of the original set of channels. To explain how polar coding exploits the idea of channel polarization, we first need to describe how the polarization transformation manufactures the channels $W_N^{(i)}$.

The first step consists of a channel combining operation. Letting X_1^N denote the inputs and Y_1^N denote the outputs of the channel W^N , we know that the transition probabilities of the super-channel describing a mapping between these two sequences, i.e., $X_1^N \rightarrow Y_1^N$, is given by

$$W^N(y_1^N | x_1^N) = \prod_{i=1}^N W(y_i | x_i), \quad (8)$$

where the product form follows from the independent use of the memoryless channel. The purpose of channel combining is to create a linear relationship between the inputs X_1^N and the inputs of the synthetic channels with the help of an intermediary super-channel of length N . Assuming U_i is the respective input to $W_N^{(i)}$, for $i = 1, \dots, N$, the polarization transformation achieves this task via a particular generator matrix G_N computed via the following recursion [1, Eq. (70)]:

$$G_N = B_N F^{\otimes N}, \quad (9)$$

where B_N is a permutation matrix known as bit-reversal, and the recursion $F^{\otimes N}$ is the N -th Kronecker product of the following 2 by 2 matrix by itself:

$$F := \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}. \quad (10)$$

The generator matrix, applied as $X_1^N = U_1^N G_N$, puts the inputs into a one-to-one correspondence, and results in a super-channel which maps this time $U_1^N \rightarrow Y_1^N$. This super-channel is denoted as $W_N : \mathbb{F}_2^N \rightarrow \mathcal{Y}^N$, and its transition probability is given by [1, Eq. (4)]:

$$W_N(y_1^N | u_1^N) = W^N(y_1^N | u_1^N G_N). \quad (11)$$

Note that in order for X_1^N to be independently and uniformly distributed, the inputs U_1^N should also be distributed as such.

Pausing for a moment here, we note that one can in principle encapsulate at this point a sequence of K -bits of information within the inputs U_1^N of length $N \geq K$ by placing each bit of information into some K coordinates of U_1^N , and by fixing the values of the remaining $(N - K)$ coordinates to some arbitrary known values. The choice of the K coordinates will determine which K rows of the matrix G_N will be used for encoding the K -bits of information before transmission over W^N . Oftentimes, coding in this context is described by the following terminology: the set of indices corresponding to the selected K rows of G_N is called the information set and is denoted by $\mathcal{A}_N \subseteq \{1, \dots, N\}$, the remaining set of indices is called the frozen set and is denoted by \mathcal{A}_N^c , and the fixed values $u_{\mathcal{A}_N^c}$ are called the frozen inputs. The encoding operation proceeds by multiplying the constructed data block with the matrix G_N to obtain the inputs X_1^N to W^N .

In the coding theory literature, an error correcting code which encodes K -bits of information in this way into an N length input to W^N is called an $(N, K, \mathcal{A}_N, u_{\mathcal{A}_N^c})$ G_N -coset code of rate K/N . For instance, Reed-Muller codes [68], [69] are one well-known family of G_N -coset codes, where the K coordinates are chosen by selecting the K rows of the matrix G_N with the K highest Hamming weights². Note that in this case, the choice of the information set \mathcal{A}_N is governed by the structure of the matrix G_N and does not depend on the given communication channel³. Polar codes are another family of G_N -coset codes in which the rule for selecting the information set is aligned with the channel polarization phenomenon observed in Theorem 1. As opposed to Reed-Muller codes, the choice of the information set of polar codes are channel dependent, and in fact, the second step following the channel combining operation, which consists of a channel splitting operation, has a key role in establishing this dependence.

Going back now where we left, we continue the discussion with this second step. Once the channels are combined as described in (11), it is possible to re-split the combined channels into a final set of N “successive” channels mapping $U_i \rightarrow Y_1^N U_1^{(i-1)}$, for $i = 1, \dots, N$. This is exactly how the polarization transformation splits the combined channels to synthesize $W_N^{(i)}$. As

²The hamming weight of a row of a binary matrix is given by the number of 1’s in it.

³The fundamental result of information theory dictates that reliable communication is only possible for communication rates less than the channel capacity. Thus a statement of the form “the information set does not depend on the given channel” should be understood in the sense that the same information set will be chosen for any channel having the same capacity regardless of the transition probability structure of the channel at hand.

a result, the transition probabilities of the synthetic channels are given by [1, Eq. (5)]:

$$W_N^{(i)}(y_1^N u_1^{i-1} | u_i) = \sum_{u_{i+1}^N \in \mathbb{F}_2^{N-i}} \frac{1}{2^{N-i}} W_N(y_1^N | u_1^N), \quad (12)$$

for $i = 1, \dots, N$.

In essence, the polarization transformation we have revisited step by step has created a communication setting (for large block-lengths) where one has access to the inputs U_i of a set of synthetic channels which are either almost perfect or almost completely noisy in the sense of the polarization effect described by Theorem 1. Polar coding exploits this phenomenon simply by defining a polar code as an $(N, K, \mathcal{A}_{N,\gamma}(W), u_{\mathcal{A}_{N,\gamma}^c(W)})$ G_N -coset code with the choice of the following information set:

$$\mathcal{A}_{N,\gamma}(W) \in \{i \in \{1, \dots, N\} : I(W_N^{(i)}) \geq 1 - \gamma\}, \quad (13)$$

for a desired threshold $\gamma \in (0, 1)$.

Due to the nature of the channel splitting operation, the input $u_i \in \mathbb{F}_2$ of the channel $W_N^{(i)}(y_1^N u_1^{i-1} | u_i)$ is a function of both the received outputs $y_1^N \in \mathcal{Y}^N$ and the previous inputs $u_1^{i-1} \in \mathbb{F}_2^{i-1}$. For this reason, polar codes lend themselves to a successive cancellation decoding procedure. The polar successive cancellation decoder, also most of the time simply called the polar decoder, decodes the received channel output sequence using a chain of estimators $\hat{u}_i \in \mathbb{F}_2$, for $i = 1, \dots, N$, where the output of each estimator depends on the estimates of the previous ones. Thus, if an error occurs at any stage, the decoder would be making its decisions on the later stages based on the probability of a wrong transition from u_i to $y_1^N \hat{u}_1^{i-1}$ with $\hat{u}_1^{i-1} \neq u_1^{i-1}$.

From the viewpoint of the individual channels, it is easy to see that while uncoded transmission would be optimal over an almost perfect channel, where no information loss occurs during transmission, any coding scheme would be useless over a completely noisy channel, since no matter how the communication scheme is designed, all the information would be lost. However, these two observations, and thus the statements in (5), (6), and (7) of Theorem 1 are not sufficient to establish a coding theorem in the context of polar coding. The performance of an $(N, K, A_N(W, \gamma), u_{A_N^c(W, \gamma)})$ polar code depends critically on the rate of channel polarization as a function of the block-length N , i.e., the speed with which the variable γ in (5), (6), and (13) can be made to approach zero as a function of N . We will further explore the results about the rate of channel polarization and its connection to the performance of the polar coding scheme,

after we first introduce in the next subsection the formal definition of a more generalized version of the polar decoder.

We close this subsection with a collection of remarks on the recursive nature of the scheme. Note that the recursion in (9) constraints the block-length to $N = 2^n$, where $n \in \mathbb{N}$ is the number of times the recursion is applied. Moreover, due to the recursive structure of the matrix G_N , the transition probabilities of the synthetic channels $W_N^{(i)}$ given in (12) can be also recursively computed, see [1, Eqs. (22) and (23), Proposition 3]. The main advantage of this special structure is that it can be implemented efficiently in $O(N \log N)$ time complexity [1, Theorem 5], while leading to channel polarization.

B. Mismatched Polar Successive Cancellation Decoder

The mismatched polar successive cancellation decoder can be described as the matched polar decoder introduced in [1] using a chain of estimators

$$\hat{u}_i = \begin{cases} u_i, & \text{if } i \in \mathcal{A}_N^c \\ f_M^{(i)}(y_1^N, \hat{u}_1^{i-1}), & \text{if } i \in \mathcal{A}_N \end{cases},$$

for $i = 1, \dots, N$, where $\mathcal{A}_N \subseteq \{1, \dots, N\}$. The difference is that the decision functions $f_M^{(i)}(y_1^N, \hat{u}_1^{i-1})$ do apply the ML rule but with respect to mismatched channels $V_N^{(i)}$ synthesized by polarizing a B-DMC V possibly different than the true communication channel W :

$$f_M^{(i)}(y_1^N, \hat{u}_1^{i-1}) := \begin{cases} 0, & \text{if } L_{V_N^{(i)}}(y_1^N, \hat{u}_1^{i-1}) < 1 \\ 1, & \text{if } L_{V_N^{(i)}}(y_1^N, \hat{u}_1^{i-1}) > 1 \\ *, & \text{if } L_{V_N^{(i)}}(y_1^N, \hat{u}_1^{i-1}) = 1 \end{cases}, \quad (14)$$

with $*$ chosen from the set $\{0, 1\}$ by a fair coin flip, and where the likelihood ratio is defined as $L_{V_N^{(i)}}(\cdot) = V_N^{(i)}(\cdot|1)/V_N^{(i)}(\cdot|0)$.

C. Code Performance: Matched vs Mismatched Setting

Let us define $P_e(W, V, \mathcal{A}_N)$ as the best achievable block decoding error probability of a G_N -coset code under mismatched polar successive cancellation decoding with respect to the channel

V when the true channel is W .⁴ Using similar derivations to the analysis carried for the matched counterpart [1, Section V], we can upper bound this error probability by:

$$\begin{aligned}
P_e(W, V, \mathcal{A}_N) &= \mathbb{P} \left[\bigcup_{i \in \mathcal{A}_N} \left\{ \hat{U}_1^{i-1} = u_1^{i-1}, \hat{U}_i \neq u_i \right\} \right] \\
&= \mathbb{P} \left[\bigcup_{i \in \mathcal{A}_N} \left\{ \hat{U}_1^{i-1} = u_1^{i-1}, f_M^{(i)}(y_1^N, \hat{U}_1^{i-1}) \neq u_i \right\} \right] \\
&\leq \mathbb{P} \left[\bigcup_{i \in \mathcal{A}_N} \left\{ f_M^{(i)}(y_1^N, u_1^{i-1}) \neq u_i \right\} \right] \\
&\leq \sum_{i \in \mathcal{A}_N} P_{e, \text{ML}}(W_N^{(i)}, V_N^{(i)}), \tag{15}
\end{aligned}$$

where

$$\begin{aligned}
P_{e, \text{ML}}(W, V) &= \sum_{\substack{y: \\ L_V(y) > 1}} W(y|0) + \frac{1}{2} \sum_{\substack{y: \\ L_V(y) = 1}} W(y|0) \\
&\quad + \sum_{\substack{y: \\ L_V(y) < 1}} W(y|1) + \frac{1}{2} \sum_{\substack{y: \\ L_V(y) = 1}} W(y|1). \tag{16}
\end{aligned}$$

It is not difficult to see that $P_{e, \text{ML}}(W, V)$ corresponds to the mismatched ML decoding error probability resulting from the single use of a B-DMC W to transmit a 0 or 1 when ML decoding with respect to a possibly mismatched B-DMC V is used as a decoding metric.

Suppose first that we are in the matched setting with $V = W$. We define $P_e(W, \mathcal{A}_N) := P_e(W, W, \mathcal{A}_N)$ and $P_{e, \text{ML}}(W) := P_{e, \text{ML}}(W, W)$. As previously discussed, at the i -th stage of decoding, to estimate the input u_i of the channel with law $W_N^{(i)}(y_1^N u_1^{i-1} | u_i)$, the polar decoder should have, in principle, correctly estimated the inputs $\hat{u}_1^{i-1} = u_1^{i-1}$ of the previous stages. Otherwise, the decoder would be computing the likelihood ratio $L_{W_N^{(i)}}(y_1^N, \hat{u}_1^{i-1})$ for the wrong outputs $\hat{u}_1^{i-1} \neq u_1^{i-1}$. Though no genie exists to give the correct estimates, [1, Theorem 3] and its strengthened version [1, Proposition 19], which we next consider, show that this decoder performs with vanishing error probability.

⁴Note that $P_e(W, V, \mathcal{A}_N)$ allows arbitrary $\mathcal{A}_N \subseteq \{1, \dots, N\}$ which are not necessarily constructed based on the rule given in (13).

Theorem 2. [1, Proposition 19] For a given B-DMC W , any fixed rate $R < I(W)$, and any constant $\beta \in (0, 1/2)$, we have

$$P_e(W, \mathcal{A}_N) = o(2^{-N^\beta}), \quad (17)$$

for any $|\mathcal{A}_N| \geq NR$ such that $\mathcal{A}_N \subseteq \mathcal{A}_{N,\gamma}(W)$ given by (13) with the choice $\gamma = o(2^{-N^\beta})$.

In order to prove this result, [1] introduces another channel parameter known as the Bhattacharyya parameter. For a B-DMC W , the Bhattacharyya parameter denoted as $Z(W)$ is given by

$$Z(W) = \sum_{y \in \mathcal{Y}} \sqrt{W(y|0)W(y|1)}, \quad (18)$$

and satisfies a well-known inequality: $P_{e, \text{ML}}(W) \leq Z(W)$. Thus, one can further upper bound $P_e(W, \mathcal{A}_N)$ in (15) with the help of the Bhattacharyya parameters of the synthetic channels as

$$P_e(W, \mathcal{A}_N) \leq \sum_{i \in \mathcal{A}_N} Z(W_N^{(i)}) \leq N \max_{i \in \mathcal{A}_N} Z(W_N^{(i)}). \quad (19)$$

The above coding theorem [1, Proposition 19] is proved by showing the following result on the rate of polarization given in terms of the Bhattacharyya parameters.

Theorem 3. [1, Proposition 18], [70, Theorems 1 and 3] For any B-DMC W , any fixed rate $R < I(W)$, and any constant $\beta \in (0, 1/2)$, there exists a sequence of sets $\mathcal{A}_N \subseteq \{1, \dots, N\}$, with $N = 2^n$ for $n \in \mathbb{N}$, such that $|\mathcal{A}_N| \geq NR$, and

$$\sum_{i \in \mathcal{A}_N} Z(W_N^{(i)}) \leq o(2^{-N^\beta}). \quad (20)$$

Conversely, if $R > 0$ and $\beta > 1/2$, then for any sequence of sets $\mathcal{A}_N \subseteq \{1, \dots, N\}$ such that $|\mathcal{A}_N| \geq NR$, we have

$$\max \left\{ Z(W_N^{(i)}) : i \in \mathcal{A}_N \right\} = \omega(2^{-N^\beta}). \quad (21)$$

To complete the proof of the coding theorem, it only remains to explore the connection of the rate of polarization result given in Theorem 3 with the speed with which the threshold γ in Theorem 1 and (13) can be made to approach zero. For this purpose, it is sufficient to study the coupling between the Bhattacharyya parameter and the symmetric capacity of a B-DMC. In that regard, the following inequalities are introduced in [1].

Proposition 1. [1, Propositions 1 and 11] For any B-DMC W ,

$$I(W)^2 + Z(W)^2 \leq 1, \quad (22)$$

$$I(W) + Z(W) \geq 1. \quad (23)$$

Thus, whenever $I(W_N^{(i)}) \geq 1 - o(2^{-N^\beta})$, we have $Z(W_N^{(i)}) \leq o(2^{-N^\beta})$, and although it is not needed in what follows, the reverse implication also follows from the given relations. Now, suppose that we design an $(N, K, \mathcal{A}_{N,\gamma}(W), u_{\mathcal{A}_{N,\gamma}(W)})$ polar code using the information set defined in (13). Then, Theorem 3 in conjunction with the coupling explored in Proposition 1 for the synthetic channels and the upper bound given in (19) imply that we can select the threshold $\gamma = o(2^{-N^\beta})$, for $\beta \in (0.1/2)$, to ensure that while the error probability is vanishing, i.e., $P_e(W, \mathcal{A}_{N,\gamma}(W)) \rightarrow 0$ as $N \rightarrow \infty$, the number of indices that remain in $\mathcal{A}_{N,\gamma}(W)$ for such a choice of γ approaches to $NI(W)$. This proves Theorem 2 which shows that polar codes with the matched polar successive cancellation decoder achieves the symmetric capacity of B-DMCs.

Let us now consider the case when $V \neq W$. We observe that even when both $W_N^{(i)}$ and $V_N^{(i)}$ are almost perfect channels with their symmetric capacities close to 1, the mismatched ML decoding error probability $P_{e, \text{ML}}(W_N^{(i)}, V_N^{(i)})$ itself may not be small; take for example, two binary symmetric channels (BSC) with crossover probabilities ϵ and $1 - \epsilon$, for $\epsilon > 0$ small. Although both channels have high symmetric capacities, the error probability is also high. Consequently, when there is mismatch in decoding, it is not clear what data rates may be achieved by the polar coding/decoding architecture, and how to design polar codes in this setting.

The effects of introducing a perturbation into the decoding procedure of the polar decoder has been considered in an earlier study [71], but diverging from this work, the study looked at the performance of an approximation to the computations of the decoder and the scope of the study was limited to BSCs. Nevertheless, the study also displays simulation results at various block-lengths of the error performance degradation introduced by the mismatched polar successive cancellation decoder doing the computations without introducing approximations for the case where W is a BSC of crossover probability 0,11 and V is a BSC of respectively 0,15/0,2/0,25/0,3 crossover probabilities. The plots in [71, Fig. 3] suggest that the error probability is still vanishing with $N \rightarrow \infty$ for mismatched pairs of BSCs.

D. A note on the dominant analysis technique used in polar coding

In the previous subsection, we stated Theorem 1 and Theorem 3 without any hint on their proofs carried in [1] and [70], respectively. In this subsection, we would like to present some of the key aspects pertaining to the analysis technique used in the proof of these theorems as we will be using a similar analysis in proving our results. However, we will also highlight certain elements of the proofs in order to showcase the similarities and differences in the application of the technique in the context of mismatched polar decoding.

One of the key ingredients in proving these theorems, and almost any result in the context of polar coding, is to exploit the recursive structure and its one-step properties inherent to the generator matrix G_N .⁵ It is customary to refer to the channel polarization transformation corresponding to the one-step application of the channel combining and splitting operations via the basic matrix F in (10) as the polar transform. For analysis purposes, it is also customary and more convenient to index the channels synthesized at the n -th level of the recursive application of the polar transform via sequences of plus and minus signs, i.e., $\{+, -\}^n$, for $n \in \mathbb{N}$. Next, we give the definition of the polar transform and the description of the synthetic channels using this alternative indexing.

From two independent copies of a given B-DMC W , the polar transform synthesizes two new B-DMCs denoted as $W^-: \mathbb{F}_2 \rightarrow \mathcal{Y}^2$ and $W^+: \mathbb{F}_2 \rightarrow \mathcal{Y}^2 \times \mathbb{F}_2$. The transition probabilities of the “minus” and “plus” channels are given by [1, Eqs. (19) and (20)]

$$W^-(y_1 y_2 | u_1) := \sum_{u_2 \in \mathbb{F}_2} \frac{1}{2} W(y_1 | u_1 \oplus u_2) W(y_2 | u_2), \quad (24)$$

$$W^+(y_1 y_2 u_1 | u_2) := \frac{1}{2} W(y_1 | u_1 \oplus u_2) W(y_2 | u_2). \quad (25)$$

Using this notation, the repeated application of the polar transform yields the following set of $N = 2^n$ synthetic channels at stage $n \in \mathbb{N}$:

$$\{W^{s^n} : s^n \in \{+, -\}^n\}. \quad (26)$$

Each of these synthetic channels corresponds to one of the channels $W_N^{(i)}: \mathbb{F}_2 \rightarrow \mathcal{Y}^N \times \mathbb{F}_2^{i-1}$, for $i = 1, \dots, N$, of the previous notation. Throughout the paper, we will alternate between the

⁵Note, however, that not all results will necessarily follow from the one-step properties of the recursion, see for instance the proof of the polarization phenomenon for non-stationary memoryless channels [49].

two notations for convenience⁶.

The following proposition summarizes the properties of the mapping $(W, W) \rightarrow (W^-, W^+)$ in terms of the symmetric capacity and the Bhattacharyya parameter.

Proposition 2. *The polar transform defined in (24) and (25) satisfies the following properties:*

1) *Polarization Property [1, Propositions 4 and 5]:*

$$I(W^-) \leq I(W) \leq I(W^+). \quad (27)$$

$$Z(W^+) \leq Z(W) \leq Z(W^-). \quad (28)$$

2) *Rate Preserving - Reliability Improving Property [1, Propositions 4 and 5]:*

$$I(W^-) + I(W^+) = 2I(W). \quad (29)$$

$$Z(W^-) + Z(W^+) \leq 2Z(W). \quad (30)$$

3) *Extremality Property [72]: It can be shown, as a corollary to extremes of information combining [73]), that among all channels W with a given symmetric capacity $I(W)$, the binary erasure channel (BEC) and the BSC polarize most and least in the sense of having the largest and the smallest differences between $I(W^+)$ and $I(W^-)$. So,*

$$I(BSC^+) - I(BSC^-) \leq I(W^+) - I(W^-) \leq I(BEC^+) - I(BEC^-). \quad (31)$$

A similar result (with reversed inequalities) can be shown for the Bhattacharyya parameters of the channels, see [74, Eqs. (61) and (62)].

4) *Local transformation of the Bhattacharyya parameter [1, Proposition 5]:*

$$Z(W^+) = Z(W)^2. \quad (32)$$

$$Z(W^-) \leq 2Z(W) - Z(W)^2. \quad (33)$$

After the single step application of the polar transform, we are easily able to compare the quality of the two synthetic channels with the original one. However, tracking the evolution of the synthetic channels in further steps is a difficult task for few reasons: the output alphabets of the channels W^{s^n} are growing exponentially fast, and there is no general total ordering between the indices $s^n \in \{+, -\}^n$ which hold for all B-DMCs due to the channel dependent evolution.

⁶In fact, it would have been more complicated to define the N -stage estimators of the polar decoder using the \pm sequence indexing.

Nevertheless, it is still possible to infer some important properties of the recursive application of the polar transform from its one-step properties. For that purpose, a useful technique is to introduce an auxiliary stochastic process called the channel polarization process.⁷

Let (Ω, \mathcal{F}, P) denote a probability space. Assume that a random i.i.d. sequence B_n , for $n \in \mathbb{N}$, defined on this space, is drawn according to a Bernoulli distribution with probabilities equal to $1/2$. Let \mathcal{F}_n be the σ -algebra generated by the collection of Bernoulli random variables B_1, \dots, B_n . The channel polarization process is defined in [1], [75] by letting $W_0 = W$ and

$$W_{n+1} := \begin{cases} W_n^-, & \text{if } B_{n+1} = 0 \\ W_n^+, & \text{if } B_{n+1} = 1 \end{cases}, \quad (34)$$

for $n \geq 0$. In this way, W_n is uniformly distributed over the set of 2^n channels. Based on the channel polarization process, one can further define additional random processes that follow the evolution of information measures as the underlying communication channel undergoes the sequence of polar transforms. Two such measures are given by the symmetric capacity process defined as $I_n(W) := I(W_n)$ and the Bhattacharyya process defined as $Z_n(W) := Z(W_n)$. Then, as shown in the next proposition, the properties of the recursive application of the polar transform can be analyzed by appealing to the theory of martingales.

Proposition 3. *The recursive application of the polar transform defined in (24) and (25) satisfies the following properties [1, Propositions 8 and 10]:*

- 1) *Boundedness:* $I_n(W)$ and $Z_n(W)$ are bounded processes on the interval $[0, 1]$.
- 2) *Martingale Law:* $I_n(W)$ is a martingale on the interval $[0, 1]$. $Z_n(W)$ is a super-martingale on the interval $[0, 1]$.
- 3) *Martingale Convergence Theorem:* $I_n(W)$ and $Z_n(W)$ are uniformly integrable processes and converges almost surely (a.s.) to limiting random variables I_∞ and Z_∞ , respectively, such that $\mathbb{E}[I_\infty] = I_0$ and $\mathbb{E}[Z_\infty] \leq Z_0$.
- 4) *Convergence Points:* $Z_\infty \in \{0, 1\}$ a.s., and similarly, $I_\infty \in \{0, 1\}$ a.s.

Let us revisit the proof of this proposition as carried out in [1].

⁷We remark that the channel polarization result of Theorem 1 can be proved without introducing such an auxiliary stochastic process, for a more elementary proof see [49, Proof of Theorem 1].

Proof: Claim 1) is straightforward since for any B-DMC, both the symmetric capacity and the Bhattacharyya parameters take values in the interval $[0, 1]$. The martingale result for $I_n(W)$ follows as the process satisfies

$$\mathbb{E}[I_n \mid \mathcal{F}_{n-1}] \quad (35)$$

$$= \mathbb{E}[I_n \mid B_1, \dots, B_{n-1}] = \mathbb{E}[I_n \mid W_{n-1}] \quad (36)$$

$$= \frac{1}{2}I(W_{n-1}^-) + \frac{1}{2}I(W_{n-1}^+) \quad (37)$$

$$= I(W_{n-1}) = I_{n-1}, \quad (38)$$

where the third equality follows by (29). Similarly, one can prove the claim for $Z_n(W)$ using the relations given in (32) and (33). Claim 3) holds by general results on bounded martingales, see for instance [76, Chapter 11]. It remains to prove the convergence points in Claim 4). Note that since $Z_n(W)$ is uniformly integrable, it also converges in \mathcal{L}_1 , and thus, $\mathbb{E}[|Z_n - Z_\infty|] \rightarrow 0$, see for instance [76, Chapter 14]. This implies that we have $\mathbb{E}[|Z_{n+1} - Z_n|] \rightarrow 0$. Since by the squaring property in (32), we can lower bound this expectation as

$$\mathbb{E}[|Z_{n+1} - Z_n|] \geq (1/2)\mathbb{E}[Z_n(1 - Z_n)] \geq 0, \quad (39)$$

it follows that $\mathbb{E}[Z_\infty(1 - Z_\infty)] \rightarrow 0$. As a result, we get $Z_\infty \in \{0, 1\}$ a.s. By the relations stated in Proposition 1, it is easy to see that $Z_\infty \in \{0, 1\}$ a.s. implies $I_\infty \in \{0, 1\}$ a.s. ■

It is worth mentioning that the convergence points of the symmetric capacity process can also be identified without the help of the Bhattacharyya process [72]. In fact, it is possible to identify the possible values I_∞ can take in a more direct way by using the extremality property stated in Proposition 2. By plotting the range of feasible $I(W)$ versus $I(W^+) - I(W^-)$ pairs using the relations in (31), it is possible to see that polarization does strictly happen, i.e., we have strict inequalities in (27), as long as $I(W)$ does not take a value at the boundary of its range. So, the synthesized channels will keep getting polarized until they hit one of the boundaries of the interval $[0, 1]$, i.e., until they become either almost perfect or almost completely noisy channels. This leads to the same conclusion that $I_\infty \in \{0, 1\}$ a.s.

The results stated for the process $I_n(W)$ in Proposition 3 prove that the recursive application of the polar transform leads to the channel polarization phenomenon observed in Theorem 1.

The results stated for the process $Z_n(W)$, on the other hand, are useful in the context of the following theorem studying the convergence properties of a more general type of tree process⁸.

Theorem 4. [70, Theorems 1 and 3] *Let Q_n be a process such that:*

(c.1) *For each $n \in \mathbb{N}$, $Q_n \in [0, 1]$, Q_0 is constant, and Q_n is measurable with respect to \mathcal{F}_n .*

Thus, Q_n is a function of B_1, \dots, B_n .

(c.2) *For some constant $q \geq 2$ and for each $n \in \mathbb{N}$,*

$$Q_{n+1} = Q_n^2, \quad \text{when } B_{n+1} = 1, \quad (40)$$

$$Q_{n+1} \leq qQ_n, \quad \text{when } B_{n+1} = 0. \quad (41)$$

(c.3) *The process Q_n converges a.s. to a $\{0, 1\}$ -valued random variable Q_∞ with $\mathbb{P}(Q_\infty = 0) = c$ for some $c \in [0, 1]$.*

Then, for any $\beta \in (0, 1/2)$,

$$\lim_{n \rightarrow \infty} \mathbb{P}[Q_n < 2^{-2^{n\beta}}] = c. \quad (42)$$

Moreover, if the condition (c.2) is replaced by the following one:

(\tilde{c} .2) *For each $n \in \mathbb{N}$,*

$$Q_{n+1} = Q_n^2, \quad \text{when } B_{n+1} = 1, \quad (43)$$

$$Q_{n+1} \geq Q_n, \quad \text{when } B_{n+1} = 0, \quad (44)$$

then, if $Q_0 > 0$, for any $\beta > 1/2$,

$$\lim_{n \rightarrow \infty} \mathbb{P}[Q_n < 2^{-2^{n\beta}}] = 0. \quad (45)$$

The rate of polarization result stated in Theorem 3 follows from Theorem 4 by letting $Q_n := Z_n(W)$, and observing that the Bhattacharyya process satisfies the conditions (c.1), (c.2), and (c.3) with $q = 2$ and $c = I(W)$, and the condition (\tilde{c} .2) with $Q_0 = Z(W) > 0$.⁹

⁸We note that [70] keeps the framework more general for the applicability of the results to more general channel polarization scenarios.

⁹Note that the case $Z(W) = 0$ is not of interest, since it corresponds to an already perfect channel, and the channel is already polarized in the sense of Theorem 1.

IV. OVERVIEW OF THE MAIN RESULTS

We introduce the main results of the paper in this section. We first give the definitions of the mismatched channel parameters that will be encountered in the remaining part of this paper. We also make few basic observations about these parameters. Then, the main results are stated in a series of theorems— Theorems 5, 6, 7, 8, and 9 — and key ideas involved in their proofs are discussed. The complete proofs are carried out in Section V.

A. Mismatched Channel Parameters

Given a B-DMC $W : \mathbb{F}_2 \rightarrow \mathcal{Y}$, we set

$$q_W(y) = \frac{W(y | 0) + W(y | 1)}{2}, \quad (46)$$

and

$$\Delta_W(y) = \frac{W(y | 0) - W(y | 1)}{W(y | 0) + W(y | 1)}, \quad (47)$$

for $y \in \mathcal{Y}$. Note that $q_W(y)$ is the output distribution of the channel when the inputs are uniformly distributed, and we have $V(y|0) = q_W(y) (1 + \Delta_V(y))$ and $V(y|1) = q_W(y) (1 - \Delta_V(y))$ ¹⁰.

Given two B-DMCs $W : \mathbb{F}_2 \rightarrow \mathcal{Y}$ and $V : \mathbb{F}_2 \rightarrow \mathcal{Y}$, the following two mismatched channel parameters are of primary interest to us in this paper: For $Y \sim q_W(y)$ with $y \in \mathcal{Y}$, we define

$$D(W, V) := \mathbb{E}[\sqrt{|\Delta_V(Y)|}] = \sum_{y \in \mathcal{Y}} q_W(y) \sqrt{|\Delta_V(y)|}, \quad (48)$$

and

$$I(W, V) := \sum_{x \in \mathbb{F}_2} \sum_{y \in \mathcal{Y}} \frac{1}{2} W(y|x) \log \frac{V(y|x)}{q_V(y)} \quad (49)$$

$$= \frac{1}{2} \sum_{y \in \mathcal{Y}} W(y|0) \log(1 + \Delta_V(y)) + \frac{1}{2} \sum_{y \in \mathcal{Y}} W(y|1) \log(1 - \Delta_V(y)). \quad (50)$$

Two other mismatched channel parameters that will be of auxiliary importance are given by

$$T(W, V) := \mathbb{E}[|\Delta_V(Y)|] = \sum_{y \in \mathcal{Y}} q_W(y) |\Delta_V(y)|, \quad (51)$$

and

$$Z(W, V) := \frac{1}{2} \sum_{y \in \mathcal{Y}} W(y|0) \sqrt{L_V(y)} + \frac{1}{2} \sum_{y \in \mathcal{Y}} W(y|1) \sqrt{\frac{1}{L_V(y)}}, \quad (52)$$

¹⁰Note that the polarization phenomenon for B-DMCs has been extensively studied via the channel parameter $\Delta_W(y)$ in [77]. A similar channel parameter and its distribution known as the Blackwell measure has also been studied later by Raginsky [78].

where we recall that $L_V(y) = V(y|1)/V(y|0)$ denotes the likelihood ratio of the channel V .

In the next three remarks, we explore the connections of the introduced mismatched channel parameters with the mismatched decoding literature, and we observe some of their basic properties.

Remark 1. Comments about $I(W, V)$:

- 1) Let us first start by mentioning that the definition of $I(W, V)$ equals the ‘generalized mutual information’ definition under the uniform input distribution in Fischer [79].¹¹ It is shown in [79] that the generalized mutual information is a lower bound on the mismatched capacity, i.e., $C(W, V) \geq I(W, V)$ holds, see also [12, Remark i)]. Thus, $|I(W, V)|^+$ is a lower bound on the mismatched capacity and an achievable rate with mismatched ML decoding.
- 2) In addition, here we show that $I(W, V)$ is also involved in an upper bound on the mismatched ML decoding error probability. Consider again a single use of the B-DMC $W: \mathbb{F}_2 \rightarrow \mathcal{Y}$ to transmit a 0. Given that the symbol 0 is transmitted, one can derive the following upper bound to the error probability resulting from such a transmission:

$$\begin{aligned}
 P_{\text{e, ML}}(W, V|0) &:= \sum_{\substack{y: \\ L_V(y) > 1}} W(y|0) + \frac{1}{2} \sum_{\substack{y: \\ L_V(y) = 1}} W(y|0) \\
 &\leq \sum_{\substack{y: \\ L_V(y) \geq 1}} W(y|0) (\log(1 + L_V(y)) - \log 2 + \log 2) \\
 &\leq 1 - \sum_{y \in \mathcal{Y}} W(y|0) \log \left(\frac{V(y|0)}{q_V(y)} \right). \tag{53}
 \end{aligned}$$

Similarly, the error probability given that the symbol 1 is transmitted can be upper bounded by

$$\begin{aligned}
 P_{\text{e, ML}}(W, V|1) &:= \sum_{\substack{y: \\ L_V(y) < 1}} W(y|1) + \frac{1}{2} \sum_{\substack{y: \\ L_V(y) = 1}} W(y|1) \\
 &\leq 1 - \sum_{y \in \mathcal{Y}} W(y|1) \log \left(\frac{V(y|0)}{q_V(y)} \right). \tag{54}
 \end{aligned}$$

¹¹Kaplan and Shamai [80] derived a more general version of Fischer’s generalized mutual information by using Gallager’s error exponent derivation technique [4], where one introduces a positive variable over which one should optimize. See also Merhav et. al. [18] for the definition of this more general expression.

Thus, when both inputs are equally likely, the average error probability satisfies

$$P_{\text{e, ML}}(W, V) = \frac{1}{2}P_{\text{e, ML}}(W, V|0) + \frac{1}{2}P_{\text{e, ML}}(W, V|1) \leq 1 - I(W, V), \quad (55)$$

where the inequality follows by (53) and (54).

- 3) It is easy to see that when $V = W$, this parameters recovers the symmetric capacity of the channel, i.e., $I(W) := I(W, W)$. For this reason, we call in this paper $I(W, V)$ as the ‘mismatched mutual information’.
- 4) It is also well known that

$$I(W) \geq I(W, V). \quad (56)$$

To see this, one can let $W_0 = W(y|0)$ and $W_1 = W(y|1)$, and simply note that the difference can be written as:

$$\begin{aligned} I(W, V) - I(W) \\ = \frac{1}{2} \text{Div}(W_0 \| V_0) + \frac{1}{2} \text{Div}(W_1 \| V_1) - \text{Div}\left(\frac{W_0 + W_1}{2} \left\| \frac{V_0 + V_1}{2}\right.\right) \geq 0, \end{aligned} \quad (57)$$

where the inequality follows from the convexity of the Kullback–Leibler divergence $\text{Div}(P_1 \| P_2)$ in the pair (P_1, P_2) [4].

- 5) By the previous result, the bound $I(W, V) \leq 1$ necessarily holds. Notice, however, that $I(W, V)$ can take on negative values, and in fact, it is unbounded from below.
- 6) If $I(W, V) = -\infty$, then there must exists at least one output symbol $y \in \mathcal{Y}$ such that $V(y|x) = 0$ but $W(y|1) > 0$. Thus, $I(W, V) = -\infty$ arises, for instance, in the case of erasures only mismatched decoding metrics for which $V(y|x) = 0$ if and only if $W(y|x) > 0$. As the name ‘erasures only’ implies, in this particular decoding procedure, the errors only come from erasures.

Remark 2. Comments about $D(W, V)$ and $T(W, V)$:

- 1) We are not aware of any previous appearance of the parameters $D(W, V)$ or $T(W, V)$ in the mismatched decoding literature.
- 2) Nevertheless, we note that the quantity $T(W, V)$ can be interpreted as a ‘mismatched variational distance’, since when $V = W$, we recover the variational distance between the distributions $W(y|0)$ and $W(y|1)$ given by

$$T(W) := T(W, W) = \frac{1}{2} \sum_{y \in \mathcal{Y}} |W(y|0) - W(y|1)|. \quad (58)$$

Similarly, when $V = W$, we recover the following alternative distance measure between the square of the distributions $W(y|0)$ and $W(y|1)$:

$$D(W) := D(W, W) = \frac{1}{2} \sum_{y \in \mathcal{Y}} |W(y|0)^2 - W(y|1)^2|. \quad (59)$$

3) Furthermore, it is possible to show the following inequalities

$$D(W, V)^2 \leq T(W, V) \leq D(W, V), \quad (60)$$

by using Jensen's inequality for concave functions and the inequality $\sqrt{x} \leq x$, for $x \in [0, 1]$, respectively.

4) Since $|\Delta_{V_n}(Y)| \in [0, 1]$ and $\sqrt{|\Delta_{V_n}(Y)|} \in [0, 1]$, it follows that both $T(W, V) \in [0, 1]$ and $D(W, V) \in [0, 1]$ hold.

Remark 3. Comments about $Z(W, V)$:

1) Skipping the proof, we first directly note that $Z(W, V)$ generates an upper bound on the mismatched ML decoding error probability as follows:

$$P_{e, \text{ML}}(W, V) \leq Z(W, V). \quad (61)$$

2) We also note that when $V = W$, this parameter recovers the channel Bhattacharyya parameter, i.e., $Z(W, W) := Z(W)$. For this reason, we call in this paper $Z(W, V)$ as the ‘mismatched Bhattacharyya parameter’.

3) However, as opposed to the Bhattacharyya parameter which satisfies $Z(W) \in [0, 1]$, here we only have $Z(W, V) \geq 0$. In fact, $Z(W, V) = \infty$, whenever $I(W, V) = -\infty$.

As we have seen in the previous section, Arıkan [1] chose to study the properties of the mapping $(W, W) \rightarrow (W^-, W^+)$ and its recursive application in terms of the symmetric capacity and the Bhattacharyya parameter for their interpretations as measures of rate and reliability, respectively, and their suitability for analysis purposes. The choice of the mismatched channel parameters, on the other hand, will be justified by the derivations and the obtained results rather than any specific interpretation of these parameters in the context of mismatched ML decoding. In other words, the mismatched channel parameters will gain idiosyncratic operational meanings along the way to the solution of the considered problem. Even though the mismatched parameters might seem as pulled out of a magic hat, recall that we have already seen with Theorem 4 that it is possible to infer results in polar coding by analyzing the behavior of certain random tree processes in a more general framework without even associating them with the channel

polarization process of a B-DMC. All in all, the identification of specific mismatched channel parameters suitable for the analysis of the mismatched polar decoder's performance shall be acknowledged as part of the main contributions of this paper.

Before we can state the theorems, we need to define the auxiliary stochastic processes corresponding to the introduced mismatched channel parameters based on the definition of the channel polarization process given in (34). We let $I_n(W, V) := I(W_n, V_n)$, $D_n(W, V) := D(W_n, V_n)$, $T_n(W, V) := T(W_n, V_n)$, and $Z_n(W, V) := Z(W_n, V_n)$ be stochastic processes associated to the channel polarization processes W_n and V_n , for $n \in \mathbb{N}$. The matched versions of these parameters are simply denoted by dropping their second argument, i.e., $I_n(W) := I_n(W, W)$, $D_n(W) := D_n(W, W)$, $T_n(W) := T_n(W, W)$, and $Z_n(W) := Z_n(W, W)$.

B. Channel Polarization in the mismatched setting

In the next theorem, we characterize the polarization phenomenon in the mismatched setting.

Theorem 5. *For any two B-DMCs $W : \mathbb{F}_2 \rightarrow \mathcal{Y}$ and $V : \mathbb{F}_2 \rightarrow \mathcal{Y}$ such that $I(W, V) > -\infty$, the mismatched pair of channels (W, V) polarize in the sense that, for all $\gamma \in (0, 1)$, we have*

$$\frac{1}{N} \#\{i \in \{1, \dots, N\} : P_{e, \text{ML}}(W_N^{(i)}, V_N^{(i)}) \in (\gamma, 1 - \gamma)\} \xrightarrow{N \rightarrow \infty} 0, \quad (62)$$

such that

$$\frac{1}{N} \#\{i \in \{1, \dots, N\} : P_{e, \text{ML}}(W_N^{(i)}, V_N^{(i)}) \in (0, \gamma]\} \xrightarrow{N \rightarrow \infty} C_P(W, V), \quad (63)$$

$$\frac{1}{N} \#\{i \in \{1, \dots, N\} : P_{e, \text{ML}}(W_N^{(i)}, V_N^{(i)}) \in [1 - \gamma, 1)\} \xrightarrow{N \rightarrow \infty} 1 - C_P(W, V), \quad (64)$$

where $N = 2^n$ with $n \in \mathbb{N}$, and $C_P(W, V) \in [0, 1]$ is defined as follows:

$$C_P(W, V) := \mathbb{P}[D_\infty(W, V) = 1]. \quad (65)$$

We remark that Theorem 5 can be seen as the mismatched counterpart of Theorem 1. In fact, one can check that for $V = W$, we have $\mathbb{P}[D_\infty(W) = 1] = \mathbb{P}[I_\infty(W) = 1]$.¹² Thus, the statement of the theorem is aligned with the original result of Theorem 1 where $C_P(W, W) = I(W) = \mathbb{P}[I_\infty(W) = 1]$. The proof of this theorem will be carried out in Section V-A. In the outline below, we highlight the important steps involved in this proof.

¹²The result can be verified by using the relation given in Lemma 11 stated in Section V-C and noting that $D_n \in [0, 1]$.

Proof Idea. The proof of the theorem will rely on the convergence properties of the mismatched processes $D_n(W, V)$ and $I_n(W, V)$ which will be investigated in Section V-A.

Regarding the process $D_n(W, V)$, we will prove in Proposition 5 that $D_n(W, V)$ is a bounded super-martingale which converges a.s. to a limiting random variable D_∞ taking values in the set $\{0, 1\}$ a.s. Let us first note that, as a consequence of such a proposition, the following polarization result readily follows: for all $\gamma \in (0, 1)$, we know that

$$\frac{1}{N} \#\{i \in \{1, \dots, N\} : D(W_N^{(i)}, V_N^{(i)}) \in (\gamma, 1 - \gamma)\} \xrightarrow{N \rightarrow \infty} 0, \quad (66)$$

such that

$$\frac{1}{N} \#\{i \in \{1, \dots, N\} : D(W_N^{(i)}, V_N^{(i)}) \in [1 - \gamma, 1)\} \xrightarrow{N \rightarrow \infty} C_P(W, V), \quad (67)$$

$$\frac{1}{N} \#\{i \in \{1, \dots, N\} : D(W_N^{(i)}, V_N^{(i)}) \in (0, \gamma]\} \xrightarrow{N \rightarrow \infty} 1 - C_P(W, V). \quad (68)$$

Although, the above three equations look similar to (62), (63), and (64), respectively, it is not clear what is the operational meaning of this particular polarization phenomenon. For this purpose, the proof of the theorem will also make use of the convergence properties of the process $I_n(W, V)$. Regarding the process $I_n(W, V)$, we will prove in Proposition 7 that the mismatched mutual information process $I_n(W, V)$ is, as its matched counterpart, a martingale process.

Using the martingale property of $I_n(W, V)$, the theorem will be proved by investigating the implications of the convergence of the mismatched process $D_n(W, V)$ on the convergence of the error probability process $P_{e, \text{ML}}(W_n, V_n)$. This coupled analysis will reveal the following operational meanings about the convergence points of the process $D_n(W, V)$ for the case where $I(W, V) > -\infty$:

- When $D_\infty = 0$ a.s., the input bits see almost completely noisy synthetic channels $W_N^{(i)}$ over which a genie aided mismatched ML decoder with respect to $V_N^{(i)}$ fails with high probability, i.e., $D_n \rightarrow 0$ as $n \rightarrow \infty$ implies $P_{e, \text{ML}}(W_n, V_n) \rightarrow 1$.
- When $D_\infty = 1$ a.s., the input bits see almost perfect synthetic channels $W_N^{(i)}$ where uncoded transmission results in a vanishing error probability under mismatched ML decoding with respect to $V_N^{(i)}$, i.e., $D_n \rightarrow 1$ as $n \rightarrow \infty$ implies $P_{e, \text{ML}}(W_n, V_n) \rightarrow 0$.

□

C. Coding Theorem with mismatched polar decoding

We saw in the previous subsection that a polarization phenomenon also holds in the mismatched setting. Theorem 5, in which we observed the polarization result in terms of the quantities $P_{\text{e, ML}}(W_N^{(i)}, V_N^{(i)})$, suggests to consider polar code constructions with the following choice of information sets:

$$\mathcal{A}_{N,\gamma}(W, V) := \{i \in \{1, \dots, N\} : P_{\text{e, ML}}(W_N^{(i)}, V_N^{(i)}) \leq \gamma\}, \quad (69)$$

where, as before, $N = 2^n$ with $n \in \mathbb{N}$ and $\gamma \in (0, 1)$ is a desired threshold. By the very definition of $P_{\text{e, ML}}(W_N^{(i)}, V_N^{(i)})$, we know that over any synthetic channel $W_N^{(i)}$ such that $i \in \mathcal{A}_{N,\gamma}(W, V)$, uncoded transmission will result in a vanishing decoding error probability even if the receiver performs mismatched ML decoding with respect to the law of the channel $V_N^{(i)}$. Moreover, for any $i \in \mathcal{A}_{N,\gamma}^c(W, V)$, transmission over $W_N^{(i)}$ will fail with high probability with the same receiver.

Although each sequence $P_{\text{e, ML}}(W_N^{(i)}, V_N^{(i)})$ vanishes for every $i \in \mathcal{A}_{N,\gamma}(W, V)$ when $N \rightarrow \infty$ and $\gamma \rightarrow 0$, whether the block decoding error probability sequence $P_{\text{e}}(W, V, \mathcal{A}_{N,\gamma}(W, V))$ of the mismatched polar successive cancellation decoder vanishes or not is still subtle. As in the matched setting, we need to investigate the rate of polarization, i.e., how fast the variable γ in (69) can be made to approach zero as a function of the block-length N . The next theorem extends the rate of convergence result of Theorem 3 to the mismatched setting.

Theorem 6. *For any two B-DMCs $W : \mathbb{F}_2 \rightarrow \mathcal{Y}$ and $V : \mathbb{F}_2 \rightarrow \mathcal{Y}$, any fixed rate $R < C_{\text{P}}(W, V)$, and constant $\beta \in (0, 1/2)$, there exists a sequence of sets $\mathcal{A}_N \subseteq \{1, \dots, N\}$, with $N = 2^n$ for $n \in \mathbb{N}$, such that $|\mathcal{A}_N| \geq NR$, and*

$$\sum_{i \in \mathcal{A}_N} P_{\text{e, ML}}(W_N^{(i)}, V_N^{(i)}) = o(2^{-N^\beta}). \quad (70)$$

The proof of this theorem will be carried out in Section V-B. Below, we present the key ideas leading to this proof.

Proof Idea. The idea of the proof will be to extend the rate of convergence claim of Theorem 4 stated in (42) to the mismatched setting by taking a closer look at the proof of this theorem carried out in [70]. We will see that the proof of the theorem does not require the conditions (c.1) and (c.3) to fully hold, and it is possible to adapt these conditions to the characteristics of the mismatched processes under consideration. Moreover, instead of identifying a suitable ‘ Q_n ’ candidate process, we will prove the theorem via a joint analysis of the processes $Z_n(W, V)$

and $D_n(W, V)$ by using their properties we will derive and ideas stemming from the proof of Theorem 5. \square

The following coding theorem follows as a corollary to Theorem 5 and Theorem 6.

Theorem 7. *For any two B-DMCs $W : \mathbb{F}_2 \rightarrow \mathcal{Y}$ and $V : \mathbb{F}_2 \rightarrow \mathcal{Y}$ such that $I(W, V) > -\infty$, and any fixed rate $R < C_P(W, V)$, there exists a sequence of information sets $\mathcal{A}_N \subseteq \{1, \dots, N\}$, for $N = 2^n$ with $n \in \mathbb{N}$, such that $|\mathcal{A}_N| \geq NR$ and*

$$Pe(W, V, \mathcal{A}_N) = o(2^{-N^\beta}). \quad (71)$$

Theorem 7, in view of Theorem 5, reveals that the quantity $C_P(W, V)$ corresponds to the transmission capacity of polar coding over the channel W when the outputs are decoded with a mismatched polar successive cancellation decoder operating with the metric of a B-DMC V which is not necessarily matched to W . We call $C_P(W, V)$ as the ‘polar mismatched capacity’.

Remark 4. In Theorem 6, we did not introduce a mismatched counterpart for the second part of Theorem 4, i.e., we did not show that a result of the form (45) holds for any $\beta > 1/2$. However, we know that if $V = W$, then (45) is true by [70, Theorem 3], since the Bhattacharyya process $Z_n(W)$ satisfies the conditions of the theorem. As by the hypothesis of Theorem 6, the channels $W : \mathbb{F}_2 \rightarrow \mathcal{Y}$ and $V : \mathbb{F}_2 \rightarrow \mathcal{Y}$ can be any two B-DMC satisfying the condition $I(W, V) > -\infty$, including the case $V = W$, we conclude that, under the general assumption of the theorem, we cannot improve the rate of convergence result stated in (108) beyond the interval $\beta \in (0, 1/2)$.

To achieve a positive rate in the mismatched setting, we note that $C_P(W, V) > 0$ must hold. The next theorem complements the previous coding theorem by providing sufficient conditions for the strict positivity of the polar mismatched capacity.

Theorem 8. *For any two B-DMCs $W : \mathbb{F}_2 \rightarrow \mathcal{Y}$ and $V : \mathbb{F}_2 \rightarrow \mathcal{Y}$, the following improving family of lower bounds on $C_P(W, V)$ holds for all $N = 2^n$ with $n \in \mathbb{N}$:*

$$C_P(W, V) \geq \frac{1}{N} \sum_{i=1}^N |I(W_N^{(i)}, V_N^{(i)})|^+. \quad (72)$$

In particular, Theorem 8 shows that positivity of the mismatched mutual information, i.e., $I(W, V) > 0$, is a sufficient condition for $C_P(W, V) > 0$. The proof of this theorem will be completed in Section V-C. We proceed with a brief discussion of the proof idea.

Proof Idea. The proof of the theorem will heavily rely on the following technical result:

$$\mathbb{P}[D_\infty(W, V) = 1] \geq I(W, V). \quad (73)$$

This result, which we will re-state in Proposition 12, will be proved in Section V-C. \square

D. From mismatched to matched setting

While the convergence speed of the Bhattacharyya process $Z_n(W)$ to the point $Z_\infty = 0$ as a function of the block-length has been investigated in [70], it was pointed out in [81] that no such result has been given for the speed of convergence to the point $Z_\infty = 1$. In the next theorem, we show that a similar rate of convergence result holds as well for the convergence of $Z_n(W)$ to $Z_\infty = 1$.

Theorem 9. *For any B-DMC W , any fixed rate $R < I(W)$, and constant $\beta \in (0, 1/2)$, there exists a sequence of sets $\mathcal{A}_N \subseteq \{1, \dots, N\}$, for $N = 2^n$ with $n \in \mathbb{N}$, such that $|\mathcal{A}_N| \geq NR$ and*

$$Z(W_N^{(i)}) \geq 1 - o(2^{-N^\beta}), \quad (74)$$

for any $i \notin \mathcal{A}_N$. Conversely, if $R > 0$ and $\beta > 1/2$, then for any sequence of sets $\mathcal{A}_N \subseteq \{1, \dots, N\}$ such that $|\mathcal{A}_N| \geq NR$, we have

$$\min \left\{ Z(W_N^{(i)}) : i \notin \mathcal{A}_N \right\} = 1 - \omega(2^{-N^\beta}). \quad (75)$$

The theorem will be proved in Section V-D. We proceed with a brief discussion of the proof idea.

Proof Idea. We will first argue in Proposition 13 that “*whenever $D_n(W, V)$ converges to zero, this converges almost surely fast*”. This argument will follow from the first part of Theorem 4 in the view of the properties we will derive for the process. Then, to show (74), we will simply need to explore the coupling between the parameters $D_\infty(W)$ and $Z_\infty(W)$. The claim in (75) will be proved similarly by using the second part of Theorem 4. This time we will explore some properties of the process $T_n(W)$, and the relation between $T_\infty(W)$ and $Z_\infty(W)$ to prove that the convergence of the process $T_n(W) \rightarrow 0$ and $Z_n(W) \rightarrow 1$ as $n \rightarrow \infty$ cannot happen faster than the $o(2^{-N^\beta})$ decay rate with $\beta \in (0, 1/2)$. \square

V. THE POLAR MISMATCHED CAPACITY

In this section, we prove Theorems 5, 6, 8, and 9. As previously, we assume that $W : \mathbb{F}_2 \rightarrow \mathcal{Y}$ and $V : \mathbb{F}_2 \rightarrow \mathcal{Y}$ denote a pair of mismatched B-DMCs.

A. Proof of Theorem 5

To prove the theorem, we first study the local transformations of the mismatched parameters $I(W, V)$ and $D(W, V)$ under the polar transform and the convergence properties of the corresponding stochastic processes $I_n(W, V)$ and $D_n(W, V)$.

The next proposition looks at the evolution of the parameter $D(W, V)$ under the polar transform.

Proposition 4. *The polar transform defined in (24) and (25) exhibits the following properties:*

$$D(W^-, V^-) = D(W, V)^2, \quad (76)$$

$$D(W^+, V^+) \leq 2D(W, V) - D(W, V)^2. \quad (77)$$

Proof: It is easy to show that

$$\Delta_{V^-}(Y_1 Y_2) = \Delta_V(Y_1) \Delta_V(Y_2), \quad (78)$$

$$\Delta_{V^+}(Y_1 Y_2 U_1) = \frac{\Delta_V(Y_1) + (-1)^{U_1} \Delta_V(Y_2)}{1 + (-1)^{U_1} \Delta_V(Y_1) \Delta_V(Y_2)}, \quad (79)$$

where $Y_1 \sim q_W(y_1)$, $Y_2 \sim q_W(y_2)$, and $U_1 | y_1 y_2 \sim \frac{1}{2} (1 + (-1)^{U_1} \Delta_W(y_1) \Delta_W(y_2))$. So, we have

$$D(W^-, V^-) = \mathbb{E} \left[\sqrt{|\Delta_{V^-}(Y_1 Y_2)|} \right] = \mathbb{E} \left[\sqrt{|\Delta_V(Y_1)|} \right] \mathbb{E} \left[\sqrt{|\Delta_V(Y_2)|} \right] = D(W, V)^2, \quad (80)$$

and

$$\begin{aligned} D(W^+, V^+) &= \mathbb{E} \left[\sqrt{|\Delta_{V^+}(Y_1 Y_2 U_1)|} \right] \\ &\leq \mathbb{E} \left[\sqrt{|\Delta_V(Y_1)|} \right] + \mathbb{E} \left[\sqrt{|\Delta_V(Y_2)|} \right] - \mathbb{E} \left[\sqrt{|\Delta_V(Y_1)|} \right] \mathbb{E} \left[\sqrt{|\Delta_V(Y_2)|} \right] \\ &= 2D(W, V) - D(W, V)^2, \end{aligned} \quad (81)$$

where the inequality holds by Lemma 1 which is stated and proved in the Appendix. ■

In the light of the local behavior uncovered by the previous proposition, we get the following result on the process $D_n(W, V)$.

Proposition 5. *The process $D_n(W, V)$ is a bounded super-martingale which converges a.s. to a limiting random variable $D_\infty(W, V)$ taking values in $\{0, 1\}$.*

Proof: By the observation in point 4) of Remark 2, we know that $D_n(W, V) \in [0, 1]$, for all $n \in \mathbb{N}$, and thus, the process is bounded. The claim that the process is a super-martingale follows

by Proposition 4 and the recursive structure of the transformation, i.e., by the observation that the recursive application of the polar transform leads to a process such that:

$$D_{n+1}(W, V) = D_n(W, V)^2, \quad \text{when } B_{n+1} = 0, \quad (82)$$

$$D_{n+1}(W, V) \leq 2D_n(W, V) - D_n(W, V)^2, \quad \text{when } B_{n+1} = 1. \quad (83)$$

By general results on bounded martingales, the process $D_n(W, V)$ is uniformly integrable, and hence it converges a.s. and in \mathcal{L}_1 to a limiting random variable $D_\infty(W, V)$ such that $\mathbb{E}[|D_n(W, V) - D_\infty(W, V)|] \rightarrow 0$ as $n \rightarrow \infty$, see for instance [76, Chapter 11]. One can prove that the convergence is to $\{0, 1\}$ using the squaring property of the minus transform given in (82) in a similar fashion as in the proof of [1, Proposition 9], where it is shown that $Z_\infty(W) \in \{0, 1\}$ a.s. See also Point 4) in Proposition 3 for a review of this derivation. ■

In the next proposition, we shift the attention to the transformation of the mismatched mutual information.

Proposition 6. *The polar transform defined in (24) and (25) preserves the mismatched mutual information of B-DMCs. i.e.,*

$$I(W^-, V^-) + I(W^+, V^+) = 2I(W, V). \quad (84)$$

Proof: In the Appendix, Lemmas 2 and 3 derive the expressions for $I(W^-, V^-)$ and $I(W^+, V^+)$, respectively. We can easily see that (84) holds, by using the expressions given in (122) and (125), respectively, and the definition of $I(W, V)$ given in (50). ■

Proposition 6 lays the foundation of another polar martingale. We now discuss this in the next proposition.

Proposition 7. *The process $I_n(W, V)$ is a martingale, where $I_n(W, V) \leq 1$ for each $n \in \mathbb{N}$. Furthermore, the process converges a.s. to a limiting random variable $I_\infty(W, V)$ such that $\mathbb{E}[I_\infty(W, V)] \geq I(W, V)$ holds.*

Proof: The martingale property follows by Proposition 6 and the recursive structure of the transformation. The claim that $I_n(W, V) \leq 1$ follows by the observation in point 5) of Remark 1. The claim about $I_\infty(W, V)$ holds by general results on bounded martingales upon noticing that $1 - I(W, V)$ is a non-negative super-martingale, see for instance [76, Section 11.7]. ■

Although the previous proposition tells us that $I_n(W, V)$ will converge a.s., it does not identify to which values the convergence will be. Let us immediately announce that we will not need

in this paper the knowledge of the limiting points of the process $I_n(W, V)$ to carry out any of the proofs. Nevertheless, it may be still worth to include a remark on this issue. Since the mismatched mutual information is unbounded from below, as opposed to the matched setting, it is not possible to get a lower bound on the difference $I(W^+, V^+) - I(W^-, V^-)$ of a similar nature to the extremal bound given in (31). In fact, it was observed in [77, Section 7.2.3] that it is possible to construct a *counter-example* to the following statement: for any $\gamma > 0$, there exists a $\xi > 0$ such that

$$|I(W, V) - I(W^-, V^-)| < \xi \quad \text{implies} \quad I(W, V) \notin (\gamma, 1 - \gamma). \quad (85)$$

Now, we are ready to prove the theorem.

Proof of Theorem 5: Using the notation introduced in (2), the definition in (16) can be equivalently written as

$$\begin{aligned} P_{\text{e, ML}}(W, V) &= W(\{y : \Delta_V(y) < 0\} | 0) + \frac{1}{2}W(\{y : \Delta_V(y) = 0\} | 0) \\ &\quad + W(\{y : \Delta_V(y) > 0\} | 1) + \frac{1}{2}W(\{y : \Delta_V(y) = 0\} | 1). \end{aligned} \quad (86)$$

Similarly, the genie-aided mismatched decoding error probability over the i -th synthetic channel can be written as

$$\begin{aligned} &P_{\text{e, ML}}(W_N^{(i)}, V_N^{(i)}) \\ &= W_N^{(i)} \left(\left\{ y_1^N u_1^{(i-1)} : \Delta_{V_N^{(i)}}(y_1^N u_1^{(i-1)}) < 0 \right\} \middle| 0 \right) + \frac{1}{2}W_N^{(i)} \left(\left\{ y_1^N u_1^{(i-1)} : \Delta_{V_N^{(i)}}(y_1^N u_1^{(i-1)}) = 0 \right\} \middle| 0 \right) \\ &\quad + W_N^{(i)} \left(\left\{ y_1^N u_1^{(i-1)} : \Delta_{V_N^{(i)}}(y_1^N u_1^{(i-1)}) > 0 \right\} \middle| 1 \right) + \frac{1}{2}W_N^{(i)} \left(\left\{ y_1^N u_1^{(i-1)} : \Delta_{V_N^{(i)}}(y_1^N u_1^{(i-1)}) = 0 \right\} \middle| 1 \right). \end{aligned}$$

We will prove the polarization results given in (66), (67), and (68), with the claim that $C_P(W, V) = \mathbb{P}[D_\infty(W, V) = 1]$, by studying the implications of the convergence properties of the process $D_n(W, V)$ on the convergence of the process $P_{\text{e, ML}}(W_n, V_n)$. Recall that, by Proposition 5, $D_\infty \in \{0, 1\}$ a.s.. We consider the two limiting cases separately:

- 1) When $D_\infty(W, V) = 0$ a.s., we first note that we also have $T_\infty(W, V) = 0$ a.s. by point 3) of Remark 2. Hence, we can write

$$T_n(W, V) = \mathbb{E}[|\Delta_{V_n}(\omega)|] \xrightarrow{n \rightarrow \infty} 0, \quad (87)$$

for $\Delta_{V_n^{s^n}}(\omega) \sim q_{W_n^{s^n}}(\omega)$, for all $s^n \in \{+, -\}^n$ with $n \in \mathbb{N}$.¹³ The convergence in (87) to 0, in turn, implies that the process

$$q_{W_n}(\{\omega : |\Delta_{V_n}(\omega)| = 0\}) \xrightarrow{n \rightarrow \infty} 1 \quad (88)$$

holds, and thus we conclude that the only possibility is to have $P_{\text{e, ML}}(W_n, V_n) \rightarrow 1$. In addition, let us also notice that the limiting random variable $I_\infty(W, V)$ can only take non-positive values here, as we have

$$\mathbb{E}[\log(1 + \Delta_{V_n}(\omega))] \leq \log(1 + \mathbb{E}[|\Delta_{V_n}(\omega)|]) \xrightarrow{n \rightarrow \infty} 0, \quad (89)$$

$$\mathbb{E}[\log(1 - \Delta_{V_n}(\omega))] \leq \log(1 - \mathbb{E}[|\Delta_{V_n}(\omega)|]) \xrightarrow{n \rightarrow \infty} 0, \quad (90)$$

by Jensen's inequality.

- 2) To analyze the case when $D_\infty(W, V) = 1$ a.s., we proceed as follows: For each of the $N = 2^n$ channels at the n -th stage of polarization, with $n \in \mathbb{N}$, we compute the probability $W_N^{(i)}\left(\left\{y_1^N u_1^{(i-1)} : \Delta_{V_N^{(i)}}\left(y_1^N u_1^{(i-1)}\right) \in [-1, -1 + \xi]\right\} \middle| 0\right)$, for any $\xi \in (0, 1)$, and for $\beta \in (0, 1)$, we let $M_n(\beta)$ be the fraction of channels for which this probability is larger than β , i.e.,

$$M_n(\beta) = \frac{1}{2^n} \#\left\{i \in \{1, \dots, N = 2^n\} : W_N^{(i)}\left(\left\{y_1^N u_1^{(i-1)} : \Delta_{V_N^{(i)}}\left(y_1^N u_1^{(i-1)}\right) \in [-1, -1 + \xi]\right\} \middle| 0\right) > \beta\right\}. \quad (91)$$

As D_n converges a.s. to a $\{0, 1\}$ -valued random variable, we note that

$$W_n(\{\omega : \Delta_{V_n}(\omega) \in (-1 + \xi, -1 + \eta)\}) \xrightarrow{n \rightarrow \infty} 0, \quad (92)$$

¹³A remark is in order for clarifying the use of the variable ω . Note that since $T_n(W, V)$ is a random process, for each $n \in \mathbb{N}$, $\mathbb{E}[|\Delta_{V_n}(\omega)|]$ is a random variable. We avoided the use of the random variables $Y_1^N U_1^{(i-1)}$, for $i = 1, \dots, N$, as an argument inside this expectation, since, while we have defined the notation $q_{W_N^{(i)}}(y_1^N u_1^{(i-1)})$ unambiguously, we have not explicitly introduced the equivalent notation with the alternative \pm indexing. That is to say, to write $q_{W_n^{s^n}}(y_1^N u_1^{(i-1)})$, for $s^n \in \{+, -\}^n$, in a consistent manner, we would have to establish first the correspondence between each index $i = 1, \dots, N$ and each $s^n \in \{+, -\}^n$. We preferred the use of the letter ω to avoid dwelling into the details of this correspondence, but one should keep in mind that, for fixed $n \in \mathbb{N}$, the quantity $\mathbb{E}[|\Delta_{V_n}(\omega)|]$ is still referring to a random variable where the randomness is over the uniformly distributed 2^n synthetic channels.

for any $\xi < \eta \in (0, 1)$; thus, the limit of $M_n(\beta)$ is independent of the choice of ξ . Furthermore, by the martingale property of $I_n(W, V)$ discussed in Proposition 7, we can write

$$\begin{aligned}
I_0 := I(W, V) &= \frac{1}{2N} \sum_{i=1}^N \sum_{\substack{y_1^N \in \mathcal{Y}^N \\ u_1^{(i-1)} \in \mathbb{F}_2}} W_N^{(i)} \left(y_1^N u_1^{(i-1)} \middle| 0 \right) \log \left(1 + \Delta_{V_N^{(i)}} \left(y_1^N u_1^{(i-1)} \right) \right) \\
&\quad + \underbrace{\frac{1}{2N} \sum_{i=1}^N \sum_{\substack{y_1^N \in \mathcal{Y}^N \\ u_1^{(i-1)} \in \mathbb{F}_2}} W_N^{(i)} \left(y_1^N u_1^{(i-1)} \middle| 1 \right) \log \left(1 - \Delta_{V_N^{(i)}} \left(y_1^N u_1^{(i-1)} \right) \right)}_{\leq \frac{1}{2} \log 2}. \quad (93)
\end{aligned}$$

Thus,

$$\begin{aligned}
I_0 &\leq \frac{1}{2} M_n(\beta) (\beta \log \xi + \log 2) + \frac{1}{2} (1 - M_n(\beta)) \log 2 + \frac{1}{2} \log 2 \\
&\leq \frac{1}{2} M_n(\beta) \beta \log \xi + \frac{3}{2} \log 2. \quad (94)
\end{aligned}$$

By the remark that the limit of $M_n(\beta)$ is not changed by the choice of ξ , we conclude that for any $\xi > 0$, $M_n(\beta)$ must vanish as $n \rightarrow \infty$, for otherwise, the right hand side of (94) will fail to be larger than $I_0 > -\infty$ for small enough ξ . As a result, we conclude that, as long as $I_0 > -\infty$, the only possibility when $D_n \rightarrow 1$ a.s. is to have $W_n(\{\omega : \Delta_{V_n}(\omega) \in (1 - \xi, 1]\} \mid 0) \rightarrow 1$. In a similar way, the argument can be repeated to show that we must have $W_n(\{\omega : \Delta_{V_n}(\omega) \in (1 - \xi, 1]\} \mid 1) \rightarrow 0$ and $W_n(\{\omega : \Delta_{V_n}(\omega) \in [-1, -1 + \xi]\} \mid 1) \rightarrow 1$ when $D_n \rightarrow 1$ a.s.. This proves that for mismatched pairs of channels (W, V) such that $I(W, V)$ is finite, the value of $P_{e, \text{ML}}(W_n, V_n)$ must be vanishing over the synthetic channels for which $D_n \rightarrow 1$ a.s. ■

B. Proof of Theorem 6

In the next proposition, we first look into how the parameters $D_n(W, V)$ and $Z_n(W, V)$ are related in general.

Proposition 8. $D(W, V) + Z(W, V) \geq 1$.

Proof: One can easily prove the inequality by using the relation

$$\Delta_V(y) = \tanh \left(\ln \left(\sqrt{\frac{1}{L_V(y)}} \right) \right), \quad (95)$$

where $\tanh(\cdot)$ denotes the hyperbolic tangent function. \blacksquare

Note that, by Proposition 8, $Z_n < \epsilon$ implies $D_n(W, V) > 1 - \epsilon$, however, the reverse implication does not hold in general for every $n \in \mathbb{N}$. Hopefully, we do not need the reverse implication to hold in general, and instead we will see that a result of weaker nature will be sufficient. The following proposition makes this statement precise.

Proposition 9. *For any $\epsilon \in (0, 1)$, there exists a $\xi \in (0, 1)$ such that*

$$\mathbb{P}[D_n(W, V) \geq 1 - \xi, Z_n(W, V) < \epsilon] \xrightarrow{n \rightarrow \infty} \mathbb{P}[D_\infty = 1]. \quad (96)$$

Proof: We claim the following:

$$\frac{1}{N} \# \left\{ i \in \{1, \dots, N = 2^n\} : D(W_N^{(i)}, V_N^{(i)}) \geq 1 - \xi, Z(W_N^{(i)}, V_N^{(i)}) \leq \sqrt{\frac{\xi}{2 - \xi}} \right\} \xrightarrow{N \rightarrow \infty} c, \quad (97)$$

where $c = \mathbb{P}[D_\infty = 1]$. As the function $f(\xi) := \sqrt{\xi/(2 - \xi)}$ takes values in the interval $(0, 1)$, for $\xi \in (0, 1)$,¹⁴ the claim in (96) follows by letting $\xi = f^{-1}(\epsilon)$, which is equivalent to $\xi = \frac{2\epsilon^2}{1 + \epsilon^2}$.

To prove the claim in (97), we explore the same idea used in the proof of Theorem 5. Using (95), we write

$$\sqrt{L_V(y)} = \sqrt{\frac{1 - \Delta_V(y)}{1 + \Delta_V(y)}}. \quad (98)$$

Then, if $\Delta_{V_N^{(i)}} \in (-1, -1 + \xi)$, we have

$$\sqrt{L_{V_N^{(i)}}} \in \left(\sqrt{\frac{2 - \xi}{\xi}}, \infty \right) \quad \text{and} \quad \sqrt{\frac{1}{L_{V_N^{(i)}}}} \in \left(0, \sqrt{\frac{\xi}{2 - \xi}} \right), \quad (99)$$

and if $\Delta_{V_N^{(i)}} \in (1 - \xi, 1)$, we have

$$\sqrt{L_{V_N^{(i)}}} \in \left(0, \sqrt{\frac{\xi}{2 - \xi}} \right) \quad \text{and} \quad \sqrt{\frac{1}{L_{V_N^{(i)}}}} \in \left(\sqrt{\frac{2 - \xi}{\xi}}, \infty \right). \quad (100)$$

Since we showed in the proof of Theorem 5 that, as long as $I(W, V) > -\infty$, $D_n \rightarrow 1$ as $n \rightarrow \infty$ implies $W_n(\{\omega : \Delta_{V_n}(\omega) \in (1 - \xi, 1]\} \mid 0) \rightarrow 1$ and $W_n(\{\omega : \Delta_{V_n}(\omega) \in [-1, -1 + \xi]\} \mid 1) \rightarrow 1$, the claim in (97) follows. \blacksquare

¹⁴ $f(\xi) \in (0, 1)$, since $f(0) = 0$, $f(1) = 1$, and $\frac{\partial f}{\partial \xi} = \frac{1}{2} \sqrt{\frac{2 - \xi}{\xi}} \frac{2}{(2 - \xi)^2} = \frac{1}{2\sqrt{\xi}(2 - \xi)^{\frac{3}{2}}} > 0$.

Next, we look into the evolution of the mismatched Bhattacharyya parameter under the one-step polar transform.

Proposition 10. *For the polar transform defined in (24) and (25), we have the following properties:*

$$Z(W^+, V^+) = Z(W, V)^2, \quad (101)$$

$$Z(W^-, V^-) \leq 2Z(W, V). \quad (102)$$

Proof: We study the evolution of $Z(W, V)$ under the polar transform:

$$\begin{aligned} Z(W^+, V^+) &= \sum_{y_1 y_2 u_1} \frac{1}{4} W(y_1|u_1) W(y_2|0) \sqrt{\frac{V(y_1|u_1 \oplus 1) V(y_2|1)}{V(y_1|u_1) V(y_2|0)}} \\ &\quad + \frac{1}{4} W(y_1|u_1 \oplus 1) W(y_2|1) \sqrt{\frac{V(y_1|u_1) V(y_2|0)}{V(y_1|u_1 \oplus 1) V(y_2|1)}} = Z(W, V)^2, \end{aligned}$$

and

$$\begin{aligned} Z(W^-, V^-) &= \sum_{y_1 y_2} \frac{1}{4} (W(y_1|0) W(y_2|0) + W(y_1|1) W(y_2|1)) \sqrt{\frac{L_V(y_1) + L_V(y_2)}{1 + L_V(y_1) L_V(y_2)}} \\ &\quad + \frac{1}{4} (W(y_1|1) W(y_2|0) + W(y_1|0) W(y_2|1)) \sqrt{\frac{1 + L_V(y_1) L_V(y_2)}{L_V(y_1) + L_V(y_2)}} \leq 2Z(W, V), \end{aligned}$$

where we used the inequalities $\sqrt{(x+y)/(1+xy)} \leq \sqrt{x} + \sqrt{y}$, $\sqrt{(1+xy)/(x+y)} \leq \sqrt{1/x} + \sqrt{y}$, and their reciprocals by replacing $x \leftarrow 1/x$ and $y \leftarrow 1/y$, for $x, y \geq 0$. ■

Now, we are ready to prove the theorem.

Proof of Theorem 6: Let us first observe that by Proposition 10, the condition (c.2) of Theorem 4 is satisfied for $Q_n := Z_n(W, V)$ with $q = 2$. However, the process $Z_n(W, V)$ fails to satisfy the conditions (c.1) and (c.3) since (i) $Z_n(W, V) \geq 1$, and (ii) we have not proved a.s. convergence¹⁵. Nevertheless, we will argue here that the first part of the theorem, i.e., the claim in (42), still holds for the process $Q_n := Z_n(W, V)$ with $q = 2$ and $c = \mathbb{P}[D_\infty = 1]$. The argument will be based on the proof of Theorem 4 carried out in [70, Section II].

At this point, we first remark that actually two alternative proofs of Theorem 4 have been presented by the authors in two different papers with the same title: Initially, the theorem and

¹⁵Note that if $Z_n(W, V)$ converges a.s., we can directly conclude via the squaring property that the only possibility is $Z_\infty(W, V) \in \{0, 1\}$ a.s., see the proof of claim 4) of Proposition 3.

its proof appeared in [75], and the proof in [70], which is of interest to us in this paper, was published later to present a simplified version of the proof of the first part of the theorem, while keeping the proof of the second part unchanged. We are highlighting this because after careful reading of both papers, one can notice that while the condition $Q_n \in [0, 1]$ is directly used in [75, Proposition 2, Lemma 1], the range of Q_n only matters in the proof presented in [70] due to the use of the function $\log Q_n$ in the derivations. Consequently, replacing the condition $Q_n \in [0, 1]$ with the condition $Q_n \geq 0$ does not affect the validity of the proof¹⁶. This solves the first problem arising from the fact that only $Z_n(W, V) \geq 0$ holds in the mismatched setting.

As for the condition $Q_\infty \in \{0, 1\}$ a.s., we remark that the proof in [70] does not make use of the fact that $Q_n \rightarrow 1$ a.s., and the condition $Q_n \rightarrow 0$ a.s. is used only to prove the following claim stated in [70, Lemma 2]: For any $\epsilon > 0$, there exists an $m \in \mathbb{N}$ such that

$$\mathbb{P} [Q_n \leq 1/q^2, \text{ for all } n \geq m] > c - \epsilon, \quad (103)$$

where $c = \mathbb{P} [Q_\infty = 0]$ and $q \geq 2$. Since the claim in (103) is the starting point of the proof carried out in [70], and the subsequent analysis proceeds without making use of the condition $Q_n \rightarrow 0$ a.s. again, we conclude that, in order to prove the claim (42) of Theorem 6, it will be sufficient to show that a result similar to (103) still holds for $Q_n := Z_n(W, V)$. We will do so by adapting the proof of [70, Lemma 2] to the current context.

More formally, we now show that for any $\epsilon > 0$, there exists an $m \in \mathbb{N}$ such that

$$\mathbb{P} [Z_n(W, V) \leq 1/q^2, \text{ for all } n \geq m] > c - \epsilon. \quad (104)$$

Since, we know that $D_\infty \in \{0, 1\}$ a.s., the definition of the constant c is unambiguous. Let $\xi(k) = f^{-1}(1/k)$, for $k \geq 1$, where the function $f(\xi) := \sqrt{\xi/(2-\xi)}$, for $\xi \in (0, 1)$, is defined as in the proof of Proposition 9. By this proposition and the definition of the limit of a sequence, we know that, for all $\epsilon > 0$, there exist a number $m \in \mathbb{N}$ such that for any $k \geq 1$, we have

$$\left| \mathbb{P} \left[Z_n(W, V) < \frac{1}{k}, D_n(W, V) \geq 1 - \xi(k), \text{ for all } n \geq m \right] - c \right| \leq \epsilon. \quad (105)$$

This, in turn, implies that

$$\mathbb{P} \left[Z_n(W, V) < \frac{1}{k}, D_n(W, V) \geq 1 - \xi(k), \text{ for all } n \geq m \right] \geq c - \epsilon. \quad (106)$$

¹⁶In addition, it is noticed in [82, Remark 1] that the squaring property is “useful” only in the sense that the repeated squaring of a number in $(\delta, 1 - \delta)$ will eventually fall outside $(\delta, 1 - \delta)$.

But, since

$$\mathbb{P} \left[Z_n(W, V) < \frac{1}{k}, \text{ for all } n \geq m \right] \geq \mathbb{P} \left[D_n(W, V) \geq 1 - \xi, Z_n(W, V) < \frac{1}{k}, \text{ for all } n \geq m \right], \quad (107)$$

the claim in (104) follows by taking $k = q^2$. Now, by replacing the claim in [70, Lemma 2] with the one in (104), we can conclude that

$$\lim_{n \rightarrow \infty} \mathbb{P}[Z_n(W, V) < 2^{-2^{n\beta}}] = c \quad (108)$$

holds for any $\beta \in (0, 1/2)$, since the remaining part of the proof follows exactly as in [70]. Let us also note that, by Proposition 8, the result in (108) implies the following:

$$\lim_{n \rightarrow \infty} \mathbb{P}[D_n(W, V) < 1 - 2^{-2^{n\beta}}] = c. \quad (109)$$

Finally, Theorem 6 follows upon noticing that, by the observation given in point 1) of Remark 3, we have

$$\sum_{i \in \mathcal{A}_N} P_{\text{e, ML}}(W_N^{(i)}, V_N^{(i)}) \leq \sum_{i \in \mathcal{A}_N} Z(W_N^{(i)}, V_N^{(i)}) = o(2^{-N^\beta}), \quad (110)$$

for any $\mathcal{A}_N \geq NR$ such that $\mathcal{A}_N \subseteq \mathcal{A}_{N,\gamma}(W, V)$ given by (69) with the choice $\gamma = o(2^{-N^\beta})$. ■

C. Proof of Theorem 8

We begin by showing a general relation between $D(W, V)$ and $I(W, V)$.

Proposition 11. $I(W, V) \leq \frac{1}{\ln 2} D(W, V)$.

Proof: The result follows from the inequalities

$$\log(1 + \Delta) \leq \sqrt{|\Delta|} / \ln 2 \quad \text{and} \quad \log(1 - \Delta) \leq \sqrt{|\Delta|} / \ln 2, \quad (111)$$

which hold for $\Delta \in [-1, 1]$. ■

We will make use of this observation to prove the following technical result.

Proposition 12. *The limiting random variable $D_\infty(W, V)$ is such that:*

$$\mathbb{P}[D_\infty(W, V) = 1] \geq I(W, V). \quad (112)$$

Proof: By Proposition 7, we know that $\mathbb{E}[I_\infty(W, V)] \geq I(W, V)$ holds. By the relation given in Proposition 11, we also know that $D_\infty(W, V) \geq I_\infty(W, V) \ln 2$ holds. On the other hand, since by Proposition 5, D_∞ is a.s. a $\{0, 1\}$ -valued random variable, we further notice that,

in fact, we have $D_\infty(W, V) \geq I_\infty(W, V)$.¹⁷ Consequently, $\mathbb{P}[D_\infty(W, V) = 1] = \mathbb{E}[D_\infty(W, V)] \geq \mathbb{E}[I_\infty(W, V)] \geq I(W, V)$, and we get the desired inequality. ■

We are now ready to complete the proof of the theorem.

Proof of Theorem 8: We have just proved in Proposition 12 that

$$\mathbb{P}[D_\infty(W, V) = 1] \geq I(W, V) \quad (113)$$

holds. Next, we discuss a trivial improvement to this lower bound. The above bound can be improved initially as $\mathbb{P}[D_\infty(W, V) = 1] \geq |I(W, V)|^+$, proving (72) for $n = 0$. Going one step further, we can improve the bound as follows:

$$\mathbb{P}[D_\infty(W, V) = 1] \geq \frac{1}{2}|I(W^-, V^-)|^+ + \frac{1}{2}|I(W^+, V^+)|^+,$$

where we used the result of Proposition 6 which shows that the quantity $I(W, V)$ is preserved under the polar transform. More generally, the bound can be improved as

$$\mathbb{P}[D_\infty(W, V) = 1] \geq \frac{1}{2^n} \sum_{s^n \in \{+, -\}^n} |I(W^{s^n}, V^{s^n})|^+,$$

for any $n \in \mathbb{N}$, by applying the same reasoning. This concludes the proof. ■

D. Proof of Theorem 9

For proving the theorem, we first investigate the rate of polarization of the process $D_n(W, V)$ to zero.

Proposition 13. *For any $\beta \in (0, 1/2)$,*

$$\lim_{n \rightarrow \infty} \mathbb{P}[D_n(W, V) < 2^{-2^{n\beta}}] = 1 - C_P(W, V). \quad (114)$$

Proof: The claims follow by [70, Theorems 1 and 3] which we restated in Theorem 4. To get (114), we simply observe that, by point 4) in Remark 2 and Propositions 4 and 5, the conditions (c.1), (c.2), and (c.3) are satisfied for the process $Q_n := D_n(W, V)$ with $c = \mathbb{P}[D_\infty(W, V) = 0] = 1 - C_P(W, V)$ and $q = 2$. ■

Now, we proceed with the proof of the theorem.

Proof of Theorem 9: In order to prove the theorem, we explore the relation between the limiting random variables $D_\infty(W)$ and $Z_\infty(W)$. It was proved in [1, Proposition 9] that

¹⁷We know that $I_\infty(W, V) \leq 1$ always holds, and obviously, we have $I_\infty(W, V) \ln 2 \leq 0$ if and only if $I_\infty(W, V) \leq 0$.

$Z_\infty(W) \in \{0, 1\}$ a.s., and we proved in Proposition 5 that, similarly, $D_\infty(W) \in \{0, 1\}$ a.s. By the relation $D_\infty(W) + Z_\infty(W) \geq 1$ given in Proposition 8, we conclude that $D_\infty(W) = 0$ if and only if $Z_\infty(W) = 1$. In view of these relations, the claim (74) of the theorem immediately follows from Proposition 13. In order to prove the second claim, we consider the process $T_n(W)$. By Point 4) of Remark 2, Proposition 5, and the relation given in (60), it is clear that the process $Q_n := T_n(W)$ satisfies the conditions (c.1) and (c.3) of Theorem 4, with $c = \mathbb{P}[T_\infty(W, V) = 0] = 1 - C_P(W, V)$ and $q = 2$. Furthermore, the condition (\tilde{c} .2) of the theorem is also satisfied, since for each $n \in N$,

$$T_{n+1} = T_n^2, \quad \text{when } B_{n+1} = 0, \quad (115)$$

$$T_{n+1} \geq T_n, \quad \text{when } B_{n+1} = 1, \quad (116)$$

where (115) follows from the product structure in (78), and (116) from [77, Lemma 6.16]. Thus, by Theorem 4, if $T(W) > 0$, then for any $\beta > 1/2$,

$$\lim_{n \rightarrow \infty} \mathbb{P}[T_n(W) < 2^{-2^{n\beta}}] = 0. \quad (117)$$

Upon noticing that $T_\infty(W) = 0$ if and only if $Z_\infty(W) = 1$, the claim in (75) follows. \blacksquare

VI. FINAL REMARKS

In this paper, we introduced the mismatched polar decoder and studied its performance in a rigorous framework. We showed that the method of polar coding can be applied in mismatched communication scenarios. The study brought a new perspective to the literature of sub-optimal ‘mismatched decoders’ and led to the concept of ‘polar mismatched capacity’. For pairs of BDMCs $W : \mathbb{F}_2 \rightarrow \mathcal{Y}$ and $V : \mathbb{F}_2 \rightarrow \mathcal{Y}$ such that $I(W, V) > -\infty$, we presented a series of theorems which uncovered the following results about the polar mismatched capacity:

- 1) The polar mismatch capacity is given by $C_P(W, V)$ which is equal to the fraction of indices for which $D_n(W, V)$ a.s. converges to 1 as $n \rightarrow \infty$,
- 2) $I(W, V)$ is a single letter lower bound on $C_P(W, V)$,
- 3) This lower bound naturally generates a sequence of tighter lower bounds on $C_P(W, V)$,
- 4) As in the matched case, the block decoding error probability of the mismatched polar decoder decays exponentially in the square root of the block-length.

We close the paper with a list of final remarks on the subject.

A. Complexity

We remark that polar coding with mismatched polar decoding uses the exact same encoding and decoding architectures proposed in [1] for the original scheme. Therefore, as explained by Arikan [1, Theorem 5], these components of the system can be implemented in $O(N \log N)$ complexity as a function of the block-length N .

Regarding the code construction, we note that the original paper [1, Section IX] proposes a Monte Carlo based approach for the construction of the information sets of the form described in (13). Initially, this raised a complexity issue regarding the construction of polar codes. Though explicitly defined, tracking the evolution of the synthetic channels is not possible in general for reasons we have already discussed. The problem of finding an efficient code construction algorithm for polar codes was first addressed by Mori and Tanaka in [83] and [84], and later these ideas were extended by Tal and Vardy [85] giving rise to an algorithm to carry out the computations approximately, but within guaranteed bounds, and efficiently. The particular case of Gaussian channels also received attention in a separate work [86] which proposed using the Gaussian approximation for computing the bit error probabilities. Beside these studies, further considerations on the complexity of polar codes revealed that the delay, construction, and decoding complexity can all be polynomially bounded as a function of the gap to capacity [87].

As in the case of the original study [1], we have not proposed an efficient algorithm to construct a polar code on the basis of the explicit definition of the information sets given in (69). While it is still possible in the mismatched setting to construct information sets of the form described in (69) via statistical methods, we believe that it should be possible to adapt the low complexity code construction algorithm proposed in [85] to the mismatched setting¹⁸.

B. List decoding of polar codes

Shortly after the inception of polar codes [1], it was discovered that the finite-length performance of the original scheme is not good enough to compete with the state-of-the-art coding schemes implemented in wireless communications systems. This result motivated a great amount

¹⁸Our claim is based on the observation that the algorithm developed in [85] is based on the fusion of probability measures [88, Chapter 1] and the fact that the channels synthesized by the polar transform are ordered by the increasing convex ordering of their Δ random variables defined in (47). See [89, Definition 2] for the definition of the increasing convex ordering, which is a partial order for B-DMCs ordering the information sets of polar codes [89, Theorem 1], [77, Corollary 6.17].

of research to focus on improving the finite-length performance of polar codes for their applicability in practical communication systems. List decoding was proposed in [90] and shown to significantly improve the finite block-length performance of polar codes. Upon this finding, the topic became one of the most active research areas in polar coding, and since, multiple list decoding algorithms and architectures have been proposed in the literature for the successive cancellation decoding of polar codes [91]–[102]. This also explains why new capacity achieving schemes that are proposed based on polar coding, such as rateless polar codes [61], present their performance results using a polar successive cancellation list decoder. Let us, however, emphasize that the primary concern of these work is to show improvements experimentally, and in fact, very limited results of theoretical nature exist regarding the performance of polar codes under list decoding.

Preliminary simulation results [103] indicate that the finite-length performance of polar codes designed for mismatched communication scenarios also improves when using a mismatched polar successive cancellation decoder implementation using a list decoding algorithm (with or without cyclic redundancy check). In the view of the state-of-the-art practice, further investigations in this area will be important to complement our work.

C. Erasures only mismatched decoding metrics

Theorem 5 and Theorem 7 give, respectively, the channel polarization result and the coding theorem for the mismatched setting under the assumption that the B-DMCs W and V are such that $I(W, V) > -\infty$. This implies that cases for which $I(W, V) = -\infty$ hold has not been treated within the scope of these theorems. By the information shared in Point 6) of Remark 1, this means that the special instance of erasure only mismatched decoding metrics are excluded from the analysis.

Suppose that the mismatch channel V is a BEC. Then, it is easy to check that $\Delta_V(y) \in \{-1, 0, 1\}$. Moreover, it is a well-known fact that the channels $V_N^{(i)}$ are also BECs [1, Proposition 6], and thus, $\Delta_{V_N^{(i)}}(y_1^N u_1^{i-1}) \in \{-1, 0, 1\}$, for any $i = 1, \dots, N$, where $N = 2^n$ with $n \in \mathbb{N}$. Now, if W is a B-DMC such that $W(y|x) > 0$ if and only if $V(y|x) = 0$, and furthermore W is a symmetric channel¹⁹ we get $D(W, V) = 1$ and $D(W_N^{(i)}, V_N^{(i)}) = 1$, while $I(W, V) = -\infty$.

¹⁹Recall that a DMC $W : \mathcal{X} \rightarrow \mathcal{Y}$ is symmetric if for some permutation π on the output alphabet \mathcal{Y} satisfying $\pi = \pi^{-1}$, we have $W(y|1) = W(\pi(y)|0)$, see for instance [4, Chapter 4].

In recent work [104], the performance trade-offs between the undetected and erasure error probabilities of polar codes decoded with a polar successive cancellation decoder with erasures have been investigated. We point out the study of the performance of polar codes with polar successive cancellation decoders using erasures only mismatched decoding metrics as an interesting area of future research.

D. Polarization as an Architecture to Boost the Classical Mismatched Capacity

The motivation of the author to study the performance of ‘mismatched decoders’ in the context of polar coding also led to the original study in [105] which investigates whether channel polarization improves the classical mismatched capacity of B-DMCs. In the study [105], channel polarization has been proposed as a novel architecture to boost the classical mismatched capacity. Let us start by revisiting an example given in that particular study.

Example 1. [105] Let W be a BSC of crossover probability $p \in (0, 0.5)$ and V be the BSC of crossover probability $1 - p$. Suppose that we apply the polar transform to synthesize the channels W^+ , W^- and V^+ , V^- . It is known that after applying the minus polar transform to a BSC of crossover probability $\alpha \in [0, 1]$, the synthesized channel is also a BSC, and with crossover probability $2\alpha(1 - \alpha)$. So, both W^- and V^- are the same BSC with crossover probability $p^- = 2p(1 - p)$. It is also easy to see that while $V^+ \neq W^+$, one has $V^{+-} = W^{+-}$, and indeed, $V^{++-} = W^{++-}$, Consequently, for any sequence $s^n \in \{-, +\}^n$ of polar transforms, $V^{s^n} = W^{s^n}$, except when $s^n = + \cdots +$. In this case $C_P(W, V) = I(W)$, and we thus have $\mathcal{A}_{N,\gamma}(W, V) = \mathcal{A}_{N,\gamma}(W, W)$, for any $\gamma > 0$.

From Example 1 and [12], [14], [17], we readily see that the specific pairs of BSCs W and V are such that $C(W, V) = 0$, while they satisfy $C_P(W, V) = I(W) > 0$. In fact, it is based on this example that [105] draws the conclusion that there exist channels for which the sequence of polar transforms strictly improve the mismatched capacity of B-DMCs, and thus, it is possible to achieve communication rates higher than $C(W, V)$ by integrating the polarization architecture [1] into the classical mismatched communication scenarios. However, [105] also argues that the conclusion is not necessarily true in general, based on the results of a numerical experiment which reveals that the quantity $C(W, V)$ can be created or lost, and is not generally preserved, after applying the polar transform to the channels W and V . Therefore, no general

order between the polar mismatched capacity $C_P(W, V)$ and the classical mismatched capacity $C(W, V)$ is formulated.

A comparison between different sub-optimal decoders may not seem to be necessarily fair, as each study corresponds to well-posed distinct mathematical problems. We stress, nevertheless, that the choice of the decoding scheme is part of the engineering problem. Since using ML decoding with the metric of a channel V or using ML with the metrics of V^- first and then V^+ in a successive cancellation decoding configuration does not differ so much in complexity for long sequences, we endorse the study [105] which conveys the message that in some cases the mismatch at the decoder can be better exploited by using the polar transform architecture of Arikan [1].

ACKNOWLEDGMENT

The author would like to thank Emre Telatar for helpful discussions and is grateful to Vincent Y. F. Tan for his comments which helped to improve the presentation of this manuscript. This work was supported by Swiss National Science Foundation under grant number 200021-125347/1, and National University of Singapore grant number R-263-000-B37-133.

APPENDIX

In this appendix, we state and prove Lemmas 1–4.

Lemma 1. *Suppose Δ_1, Δ_2 are independent $[-1, 1]$ valued random variables with $\mathbb{E} [\sqrt{|\Delta_i|}] = \mu_i$. Then*

$$\mathbb{E} \left[\sqrt{\left| \frac{\Delta_1 + \Delta_2}{1 + \Delta_1 \Delta_2} \right|} \right] \leq \mu_1 + \mu_2 - \mu_1 \mu_2, \quad (118)$$

and

$$\mathbb{E} \left[\sqrt{\left| \frac{\Delta_1 - \Delta_2}{1 - \Delta_1 \Delta_2} \right|} \right] \leq \mu_1 + \mu_2 - \mu_1 \mu_2. \quad (119)$$

Proof: If we take $a = \sqrt{|\Delta_1|}$ and $b = \sqrt{|\Delta_2|}$ in Lemma 4 which is given at the end of this appendix, note that we get the following inequalities:

$$\sqrt{\left| \frac{\Delta_1 + \Delta_2}{1 + \Delta_1 \Delta_2} \right|} \leq \sqrt{|\Delta_1|} + \sqrt{|\Delta_2|} - \sqrt{|\Delta_1|} \sqrt{|\Delta_2|}, \quad (120)$$

and

$$\sqrt{\left| \frac{\Delta_1 - \Delta_2}{1 - \Delta_1 \Delta_2} \right|} \leq \sqrt{|\Delta_1|} + \sqrt{|\Delta_2|} - \sqrt{|\Delta_1|} \sqrt{|\Delta_2|}. \quad (121)$$

Now, by taking expectations of both sides of (120) and (121), and noting the independence of Δ_1 and Δ_2 , the claims (118) and (119) of the lemma follow. \blacksquare

Lemma 2. *Let $W : \mathbb{F}_2 \rightarrow \mathcal{Y}$ and $V : \mathbb{F}_2 \rightarrow \mathcal{Y}$ be two B-DMCs. Then,*

$$\begin{aligned} I(W^-, V^-) &= \frac{1}{4} \sum_{y_1 y_2 \in \mathcal{Y}^2} W(y_1|0)W(y_2|0) \log(1 + \Delta_V(y_1)\Delta_V(y_2)) \\ &\quad + \frac{1}{4} \sum_{y_1 y_2 \in \mathcal{Y}^2} W(y_1|0)W(y_2|1) \log(1 - \Delta_V(y_1)\Delta_V(y_2)) \\ &\quad + \frac{1}{4} \sum_{y_1 y_2 \in \mathcal{Y}^2} W(y_1|1)W(y_2|0) \log(1 - \Delta_V(y_1)\Delta_V(y_2)) \\ &\quad + \frac{1}{4} \sum_{y_1 y_2 \in \mathcal{Y}^2} W(y_1|1)W(y_2|1) \log(1 + \Delta_V(y_1)\Delta_V(y_2)). \end{aligned} \quad (122)$$

Proof: Using the definition of the minus transformation in (24), the proof follows upon observing that the following relations hold:

$$1 + \Delta_V(y_1)\Delta_V(y_2) = \frac{2V(y_1|0)V(y_2|0) + 2V(y_1|1)V(y_2|1)}{\sum_{u \in \mathbb{F}_2} V(y_1|u)V(y_2|u) + V(y_1|u \oplus 1)V(y_2|u)}, \quad (123)$$

$$1 - \Delta_V(y_1)\Delta_V(y_2) = \frac{2V(y_1|0)V(y_2|1) + 2V(y_1|1)V(y_2|0)}{\sum_{u \in \mathbb{F}_2} V(y_1|u)V(y_2|u) + V(y_1|u \oplus 1)V(y_2|u)}. \quad (124)$$

\blacksquare

Lemma 3. *Let $W : \mathbb{F}_2 \rightarrow \mathcal{Y}$ and $V : \mathbb{F}_2 \rightarrow \mathcal{Y}$ be two B-DMCs. Then,*

$$\begin{aligned} I(W^+, V^+) &= \frac{1}{4} \sum_{y_1 y_2 \in \mathcal{Y}^2} W(y_1|0)W(y_2|0) \log \left(1 + \frac{\Delta_V(y_1) + \Delta_V(y_2)}{1 + \Delta_V(y_1)\Delta_V(y_2)} \right) \\ &\quad + \frac{1}{4} \sum_{y_1 y_2 \in \mathcal{Y}^2} W(y_1|0)W(y_2|1) \log \left(1 + \frac{\Delta_V(y_1) - \Delta_V(y_2)}{1 - \Delta_V(y_1)\Delta_V(y_2)} \right) \\ &\quad + \frac{1}{4} \sum_{y_1 y_2 \in \mathcal{Y}^2} W(y_1|1)W(y_2|0) \log \left(1 - \frac{\Delta_V(y_1) - \Delta_V(y_2)}{1 - \Delta_V(y_1)\Delta_V(y_2)} \right) \\ &\quad + \frac{1}{4} \sum_{y_1 y_2 \in \mathcal{Y}^2} W(y_1|1)W(y_2|1) \log \left(1 - \frac{\Delta_V(y_1) + \Delta_V(y_2)}{1 + \Delta_V(y_1)\Delta_V(y_2)} \right). \end{aligned} \quad (125)$$

Proof: Using the definition of the plus transformation in (25), the proof follows upon

observing

$$1 + \frac{\Delta_V(y_1) + \Delta_V(y_2)}{1 + \Delta_V(y_1)\Delta_V(y_2)} = \frac{2V(y_1|0)V(y_2|0)}{\sum_{u \in \mathbb{F}_2} V(y_1|u)V(y_2|u)}, \quad (126)$$

$$1 - \frac{\Delta_V(y_1) + \Delta_V(y_2)}{1 + \Delta_V(y_1)\Delta_V(y_2)} = \frac{2V(y_1|1)V(y_2|1)}{\sum_{u \in \mathbb{F}_2} V(y_1|u)V(y_2|u)}, \quad (127)$$

$$1 + \frac{\Delta_V(y_1) - \Delta_V(y_2)}{1 - \Delta_V(y_1)\Delta_V(y_2)} = \frac{2V(y_1|0)V(y_2|1)}{\sum_{u \in \mathbb{F}_2} V(y_1|u)V(y_2|u \oplus 1)}, \quad (128)$$

$$1 - \frac{\Delta_V(y_1) - \Delta_V(y_2)}{1 - \Delta_V(y_1)\Delta_V(y_2)} = \frac{2V(y_1|1)V(y_2|0)}{\sum_{u \in \mathbb{F}_2} V(y_1|u)V(y_2|u \oplus 1)}. \quad (129)$$

■

Lemma 4. For a, b in the interval $[0, 1]$,

$$\sqrt{\frac{|a^2 - b^2|}{1 - a^2b^2}} \leq \sqrt{\frac{a^2 + b^2}{1 + a^2b^2}} \leq a + b - ab.$$

Proof: For the first inequality, we can assume without loss of generality that $x = a^2 \geq b^2 = y$, and we only need to check

$$\frac{x - y}{1 - xy} \leq \frac{x + y}{1 + xy}, \quad (130)$$

for $x, y \in [0, 1]$, or equivalently, $(x - y)(1 + xy) \leq (x + y)(1 - xy)$. But this last simplifies to $x^2y \leq y$, which clearly holds.

For the second inequality, squaring both sides and multiplying by $(1 + a^2b^2)$ we see that the inequality is equivalent to

$$(a + b - ab)^2(1 + a^2b^2) - a^2 - b^2 \geq 0. \quad (131)$$

The left hand side factorizes as $a(1 - a)b(1 - b)(2 - ab(1 + a + b - ab))$. Thus the lemma will be proved once we show that

$$t(1 + s - t) \leq 2, \quad (132)$$

where $s = a + b$ and $t = ab$. Note that $0 \leq s \leq 2$ and $0 \leq t \leq 1$. Thus, $t(1 + s - t) \leq t(3 - t) \leq 2$.

■

REFERENCES

- [1] E. Arkan, "Channel polarization: A method for constructing capacity-achieving codes for symmetric binary-input memoryless channels," *IEEE Trans. Inf. Theory*, vol. 55, no. 7, pp. 3051–3073, 2009.
- [2] J. Salz and E. Zehavi, "Decoding under integer metrics constraints," *IEEE Trans. on Comm.*, vol. 43, no. 2/3/4, pp. 307–317, Feb 1995.
- [3] C. E. Shannon, "A mathematical theory of communication," *Bell System Technical Journal*, vol. 27, no. 3, pp. 379–423, 1948.
- [4] R. G. Gallager, *Information Theory and Reliable Communication*. New York, NY, USA: John Wiley & Sons, Inc., 1968.
- [5] I. Csiszár, J. Körner, and K. Marton, "A new look at the error exponent of coding for discrete memoryless channels," *Proc. of the IEEE Int. Symp. on Inf. Theory (ISIT)*, 1977.
- [6] I. Csiszár and J. Körner, *Information Theory: Coding Theorems for Discrete Memoryless Systems*. Orlando, FL, USA: Academic Press, Inc., 1982.
- [7] V. D. Goppa, "Nonprobabilistic mutual information without memory," *Probl. Contr. Inform. Theory*, vol. 4, pp. 97–102, 1975.
- [8] I. Csiszár, "The method of types [information theory]," *IEEE Trans. Inf. Theory*, vol. 44, no. 6, pp. 2505–2523, 1998.
- [9] D. J. Costello and J. Forney, G. D., "Channel coding: The road to channel capacity," *Proc. of the IEEE*, vol. 95, no. 6, pp. 1150–1177, 2007.
- [10] E. Arıkan, "On the origin of polar coding," *IEEE Journal on Selected Areas in Comm. (JSAC)*, vol. 34, no. 2, pp. 209–223, Feb 2016.
- [11] I. Csiszár and J. Körner, "Graph decomposition: A new key to coding theorems," *IEEE Trans. Inf. Theory*, vol. 27, no. 1, pp. 5–12, 1981.
- [12] I. Csiszár and P. Narayan, "Channel capacity for a given decoding metric," *IEEE Trans. Inf. Theory*, vol. 41, no. 1, pp. 35–43, 1995.
- [13] C. E. Shannon, "The zero error capacity of a noisy channel," *IRE Trans. Inf. Theory*, vol. 2, no. 3, pp. 8–19, 1956.
- [14] V. B. Balakirsky, "Coding theorem for discrete memoryless channels with given decision rule," *Proceedings of the First French-Soviet Workshop on Algebraic Coding*, pp. 142–150, Jul. 1991.
- [15] —, "A converse coding theorem for mismatched decoding at the output of binary-input memoryless channels," *IEEE Trans. Inf. Theory*, vol. 41, no. 6, pp. 1889–1902, 1995.
- [16] J. Scarlett, A. Somekh-Baruch, A. Martinez, and A. Guillen i Fabregas, "A counter-example to the mismatched decoding converse for binary-input discrete memoryless channels," *IEEE Trans. Inf. Theory*, vol. PP, no. 99, pp. 1–1, 2015.
- [17] J. Y. N. Hui, "Fundamental issues of multiple accessing," Ph.D. dissertation, MIT, 1983.
- [18] N. Merhav, G. Kaplan, A. Lapidoth, and S. Shamai Shitz, "On information rates for mismatched decoders," *IEEE Trans. Inf. Theory*, vol. 40, no. 6, pp. 1953–1967, 1994.
- [19] A. Lapidoth, "Mismatched decoding and the multiple-access channel," *IEEE Trans. on Inf. Theory*, vol. 42, no. 5, pp. 1439–1452, Sep 1996.
- [20] —, "Nearest neighbor decoding for additive non-gaussian noise channels," *IEEE Trans. on Inf. Theory*, vol. 42, no. 5, pp. 1520–1529, Sep 1996.
- [21] G. Forney, "Exponential error bounds for erasure, list, and decision feedback schemes," *IEEE Trans. on Inf. Theory*, vol. 14, no. 2, pp. 206–220, Mar 1968.
- [22] M. S. Pinsker and A. Y. Sheverdyaev, "Transmission capacity with zero error and erasure," *Probl. Peredach. Inform.*, vol. 6, no. 1, pp. 20–24, 1970.

- [23] R. Ahlswede, N. Cai, and Z. ZHANG, "Erasure, list, and detection zero-error capacities for low noise and a relation to identification," *IEEE Trans. on Inf. Theory*, vol. 42, no. 1, pp. 55–62, Jan 1996.
- [24] I. E. Telatar and R. G. Gallager, "New exponential upper bounds to error and erasure probabilities," in *Proc. of the IEEE Int. Symp. on Inf. Theory (ISIT)*, Jun 1994, pp. 379–.
- [25] A. Ganti, A. Lapidoth, and I. Telatar, "Mismatched decoding revisited: general alphabets, channels with memory, and the wide-band limit," *IEEE Trans. on Inf. Theory*, vol. 46, no. 7, pp. 2315–2328, Nov 2000.
- [26] C. Bunte, A. Lapidoth, and A. Samorodnitsky, "The zero-undetected-error capacity approaches the sperner capacity," *CoRR*, vol. abs/1309.4930, 2013. [Online]. Available: <http://arxiv.org/abs/1309.4930>
- [27] J. Scarlett, A. Martinez, and A. G. i. Fabregas, "Mismatched decoding: Error exponents, second-order rates and saddlepoint approximations," *IEEE Trans. on Inf. Theory*, vol. 60, no. 5, pp. 2647–2666, May 2014.
- [28] A. Somekh-Baruch, "On achievable rates and error exponents for channels with mismatched decoding," *IEEE Trans. on Inf. Theory*, vol. 61, no. 2, pp. 727–740, Feb 2015.
- [29] J. Scarlett, A. Martinez, and A. G. i. Fàbregas, "Multiuser random coding techniques for mismatched decoding," *IEEE Trans. on Inf. Theory*, vol. 62, no. 7, pp. 3950–3970, July 2016.
- [30] A. Somekh-Baruch, "A general formula for the mismatch capacity," *IEEE Trans. on Inf. Theory*, vol. 61, no. 9, pp. 4554–4568, Sept 2015.
- [31] J. Scarlett, V. Y. F. Tan, and G. Durisi, "The dispersion of nearest-neighbor decoding for additive non-gaussian channels," in *Proc. of the IEEE Int. Symp. on Inf. Theory (ISIT)*, July 2016, pp. 2664–2668.
- [32] J. Scarlett, "Reliable communication under mismatch decoding," Ph.D. dissertation, Cambridge, 2014.
- [33] C. Leroux, A. J. Raymond, G. Sarkis, and W. J. Gross, "A semi-parallel successive-cancellation decoder for polar codes," *IEEE Trans. on Sig. Process.*, vol. 61, no. 2, pp. 289–299, Jan 2013.
- [34] A. J. Raymond and W. J. Gross, "A scalable successive-cancellation decoder for polar codes," *IEEE Trans. on Sig. Process.*, vol. 62, no. 20, pp. 5339–5347, Oct 2014.
- [35] O. Dizdar and E. Arıkan, "A high-throughput energy-efficient implementation of successive cancellation decoder for polar codes using combinational logic," *IEEE Trans. on Circuits and Systems I: Regular Papers*, vol. 63, no. 3, pp. 436–447, March 2016.
- [36] E. Şaşıoğlu, "Polar coding theorems for discrete systems," Ph.D. dissertation, Lausanne, 2011.
- [37] E. Abbe and E. Telatar, "Polar codes for the m-user multiple access channel," *IEEE Trans on Inf. Theory*, vol. 58, no. 8, pp. 5437–5448, Aug 2012.
- [38] W. Park and A. Barg, "Polar codes for q-ary channels, $q = 2^n$," *IEEE Trans. on Inf. Theory*, vol. 59, no. 2, pp. 955–969, Feb 2013.
- [39] A. G. Sahebi and S. S. Pradhan, "Multilevel channel polarization for arbitrary discrete memoryless channels," *IEEE Trans. on Inf. Theory*, vol. 59, no. 12, pp. 7839–7857, Dec 2013.
- [40] R. Nasser and E. Telatar, "Polar codes for arbitrary dmcs and arbitrary macs," *IEEE Trans. on Inf. Theory*, vol. 62, no. 6, pp. 2917–2936, June 2016.
- [41] E. Abbe and A. Barron, "Polar coding schemes for the awgn channel," in *Proc. of the IEEE Int. Symp. on Inf. Theory*, July 2011, pp. 194–198.
- [42] D. Sutter, J. M. Renes, F. Dupuis, and R. Renner, "Achieving the capacity of any dmc using only polar codes," in *Proc. of the IEEE Inf. Theory Workshop (ITW)*, Sept 2012, pp. 114–118.
- [43] M. Andersson, V. Rathi, R. Thobaben, J. Kliewer, and M. Skoglund, "Nested polar codes for wiretap and relay channels," *IEEE Comm. Letters*, vol. 14, no. 8, pp. 752–754, August 2010.

- [44] N. Goela, E. Abbe, and M. Gastpar, "Polar codes for broadcast channels," *IEEE Trans on Inf. Theory*, vol. 61, no. 2, pp. 758–782, Feb 2015.
- [45] M. Mondelli, S. H. Hassani, I. Sason, and R. L. Urbanke, "Achieving marton's region for broadcast channels using polar codes," *IEEE Trans on Inf. Theory*, vol. 61, no. 2, pp. 783–800, Feb 2015.
- [46] R. A. Chou and M. R. Bloch, "Polar coding for the broadcast channel with confidential messages: A random binning analogy," *IEEE Trans on Inf. Theory*, vol. 62, no. 5, pp. 2410–2429, May 2016.
- [47] M. M. Wilde and S. Guha, "Polar codes for degradable quantum channels," *IEEE Trans. on Inf. Theory*, vol. 59, no. 7, pp. 4718–4729, July 2013.
- [48] —, "Polar codes for classical-quantum channels," *IEEE Trans. on Inf. Theory*, vol. 59, no. 2, pp. 1175–1187, Feb 2013.
- [49] M. Alsan and E. Telatar, "A simple proof of polarization and polarization for non-stationary memoryless channels," *IEEE Trans. on Inf. Theory*, vol. 62, no. 9, pp. 4873–4878, Sept 2016.
- [50] H. Si, O. O. Koyluoglu, and S. Vishwanath, "Polar coding for fading channels: Binary and exponential channel cases," *IEEE Trans. on Comm.*, vol. 62, no. 8, pp. 2638–2650, Aug 2014.
- [51] S. L. Fong and V. Y. F. Tan, "On the scaling exponent of polar codes for binary-input energy-harvesting channels," *IEEE Journal on Selected Areas in Comm. (JSAC)*, vol. PP, no. 99, pp. 1–1, 2016.
- [52] M. Seidl, A. Schenk, C. Stierstorfer, and J. B. Huber, "Polar-coded modulation," *IEEE Trans. on Comm.*, vol. 61, no. 10, pp. 4108–4119, October 2013.
- [53] H. Mahdaviifar and A. Vardy, "Achieving the secrecy capacity of wiretap channels using polar codes," *IEEE Trans on Inf. Theory*, vol. 57, no. 10, pp. 6428–6443, Oct 2011.
- [54] O. O. Koyluoglu and H. E. Gamal, "Polar coding for secure transmission and key agreement," *IEEE Trans on Inf. Forensics and Security*, vol. 7, no. 5, pp. 1472–1483, Oct 2012.
- [55] E. Abbe, "Randomness and dependencies extraction via polarization, with applications to slepian-wolf coding and secrecy," *IEEE Trans on Inf. Theory*, vol. 61, no. 5, pp. 2388–2398, May 2015.
- [56] R. A. Chou, M. R. Bloch, and E. Abbe, "Polar coding for secret-key generation," *IEEE Trans on Inf. Theory*, vol. 61, no. 11, pp. 6213–6237, Nov 2015.
- [57] Y. P. Wei and S. Ulukus, "Polar coding for the general wiretap channel with extensions to multiuser scenarios," *IEEE Journal on Selected Areas in Comm. (JSAC)*, vol. 34, no. 2, pp. 278–291, Feb 2016.
- [58] D. Burshtein and A. Struagatski, "Polar write once memory codes," *IEEE Trans. on Inf. Theory*, vol. 59, no. 8, pp. 5088–5101, Aug 2013.
- [59] B. Peleato, R. Agarwal, J. M. Cioffi, M. Qin, and P. H. Siegel, "Adaptive read thresholds for nand flash," *IEEE Trans. on Comm.*, vol. 63, no. 9, pp. 3069–3081, Sept 2015.
- [60] E. E. Gad, Y. Li, J. Kliewer, M. Langberg, A. A. Jiang, and J. Bruck, "Asymmetric error correction and flash-memory rewriting using polar codes," *IEEE Trans. on Inf. Theory*, vol. 62, no. 7, pp. 4024–4038, July 2016.
- [61] B. Li, D. Tse, K. Chen, and H. Shen, "Capacity-achieving rateless polar codes," in *Proc. of the IEEE Int Symp. on Inf. Theory (ISIT)*, July 2016, pp. 46–50.
- [62] S. N. Hong, D. Hui, and I. Marić, "Capacity-achieving rate-compatible polar codes," in *Proc. of the IEEE Int. Symp. on Inf. Theory (ISIT)*, July 2016, pp. 41–45.
- [63] S. B. Korada, "Polar codes for channel and source coding," Ph.D. dissertation, Lausanne, 2009.
- [64] E. Arıkan, "Source polarization," in *Proc. of the IEEE Int. Symp. on Inf. Theory (ISIT)*, June 2010, pp. 899–903.
- [65] —, "Polar coding for the slepian-wolf problem based on monotone chain rules," in *Proc. of the IEEE Int. Symp. on Inf. Theory (ISIT)*, July 2012, pp. 566–570.

- [66] M. Karzand and E. Telatar, "Polar codes for q-ary source coding," in *Proc. of the IEEE Int. Symp. on Inf. Theory (ISIT)*, June 2010, pp. 909–912.
- [67] R. Mori and T. Tanaka, "Source and channel polarization over finite fields and reed-solomon matrices," *IEEE Trans. on Inf. Theory*, vol. 60, no. 5, pp. 2720–2736, May 2014.
- [68] D. E. Muller, "Application of boolean algebra to switching circuit design and to error correction," *IRE Trans. Electron. Comput.*, vol. EC-3, no. 9, pp. 6–12, Sep. 1954.
- [69] I. Reed, "A class of multiple-error-correcting codes and the decoding scheme," *IRE Trans. Inf. Theory*, vol. IT-4, no. 3, p. 39–44, Sep. 1954.
- [70] E. Arıkan and I. E. Telatar, "On the rate of channel polarization," pp. 1493–1495, 2009.
- [71] M. Alsan, "Performance of mismatched polar codes over BSCs," in *Proc. of Int. Symp. on Inf. Theory and its App. (ISITA)*, Oct 2012, pp. 750–755.
- [72] E. Telatar, "Polarization codes and the rate of polarization," Sep. 2008, at publication date slides of the lecture are available online at. [Online]. Available: <http://ipg.epfl.ch/leveque/Seminar/telatar.pdf>
- [73] I. Sutskever, S. Shamaï, and J. Ziv, "Extremes of information combining," *IEEE Trans. Inf. Theory*, vol. 51, no. 4, pp. 1313–1325, 2005.
- [74] M. Alsan, "Extremal channels of Gallager's E_0 under the basic polarization transformations," *IEEE Trans. on Inf. Theory*, vol. 60, no. 3, pp. 1582–1591, March 2014.
- [75] E. Arıkan and E. Telatar, "On the rate of channel polarization," *CoRR*, vol. abs/0807.3806, 2008. [Online]. Available: <http://arxiv.org/abs/0807.3806>
- [76] D. Williams, *Probability with Martingales*, ser. Cambridge mathematical textbooks. Cambridge University Press, 1991.
- [77] M. Alsan, "Re-proving channel polarization theorems: an extremality and robustness analysis," Ph.D. dissertation, EPFL, 2015.
- [78] M. Raginsky, "Channel polarization and blackwell measures," in *Proc. of the IEEE Int Symp. on Inf. Theory (ISIT)*, July 2016, pp. 56–60.
- [79] T. R. M. Fischer, "Some remarks on the role of inaccuracy in Shannon's theory of information transmission," in *Trans. of the Eighth Prague Conference*, ser. Czechoslovak Academy of Sciences. Springer Netherlands, 1978, vol. 8A, pp. 211–226.
- [80] G. Kaplan and S. Shamaï, "Information rates and error exponents of compound channels with application to antipodal signaling in a fading environment," *A&U*, vol. 47, no. 4, pp. 228–239, 1993.
- [81] I. Tal, "Polar coding for processes with memory," July. 2016, talk presented in the IEEE International Symposium on Information Theory (ISIT).
- [82] E. Şaşıoğlu, E. Telatar, and E. Arıkan, "Polarization for arbitrary discrete memoryless channels," *CoRR*, vol. abs/0908.0302, 2009. [Online]. Available: <http://arxiv.org/abs/0908.0302>
- [83] R. Mori and T. Tanaka, "Performance and construction of polar codes on symmetric binary-input memoryless channels," in *Proc. of the IEEE Int. Symp. on Inf. Theory (ISIT)*, June 2009, pp. 1496–1500.
- [84] —, "Performance of polar codes with the construction using density evolution," *Communications Letters, IEEE*, vol. 13, no. 7, pp. 519–521, July 2009.
- [85] I. Tal and A. Vardy, "How to construct polar codes," *IEEE Trans. Inf. Theory*, vol. 59, no. 10, pp. 6562–6582, 2013.
- [86] P. Trifonov, "Efficient design and decoding of polar codes," *IEEE Trans on Comm.*, vol. 60, no. 11, pp. 3221–3227, November 2012.
- [87] V. Guruswami and P. Xia, "Polar codes: Speed of polarization and polynomial gap to capacity," *IEEE Trans. on Inf. Theory*, vol. 61, no. 1, pp. 3–16, Jan 2015.

- [88] R. Szekli, *Stochastic ordering and dependence in applied probability*, ser. Lecture notes in statistics. Springer-Verlag, 1995.
- [89] M. Alsan, "A novel partial order for the information sets of polar codes over b-dmcs," in *2014 IEEE International Symposium on Information Theory*, June 2014, pp. 136–140.
- [90] I. Tal and A. Vardy, "List decoding of polar codes," in *Proc. of the IEEE Int. Symp. on Inf. Theory (ISIT)*, 2011, pp. 1–5.
- [91] —, "List decoding of polar codes," *IEEE Trans. on Inf. Theory*, vol. 61, no. 5, pp. 2213–2226, May 2015.
- [92] B. Li, H. Shen, and D. Tse, "An adaptive successive cancellation list decoder for polar codes with cyclic redundancy check," *IEEE Comm. Letters*, vol. 16, no. 12, pp. 2044–2047, December 2012.
- [93] C. Zhang and K. K. Parhi, "Low-latency sequential and overlapped architectures for successive cancellation polar decoder," *IEEE Trans. on Signal Processing*, vol. 61, no. 10, pp. 2429–2441, May 2013.
- [94] K. Chen, K. Niu, and J. Lin, "Improved successive cancellation decoding of polar codes," *IEEE Trans. on Comm.*, vol. 61, no. 8, pp. 3100–3107, August 2013.
- [95] A. Balatsoukas-Stimming, A. J. Raymond, W. J. Gross, and A. Burg, "Hardware architecture for list successive cancellation decoding of polar codes," *IEEE Trans. on Circuits and Systems II: Express Briefs*, vol. 61, no. 8, pp. 609–613, Aug 2014.
- [96] A. Balatsoukas-Stimming, M. B. Parizi, and A. Burg, "Llr-based successive cancellation list decoding of polar codes," *IEEE Trans. on Signal Processing*, vol. 63, no. 19, pp. 5165–5179, Oct 2015.
- [97] Z. Zhang, L. Zhang, X. Wang, C. Zhong, and H. V. Poor, "A split-reduced successive cancellation list decoder for polar codes," *IEEE Journal on Selected Areas in Comm. (JSAC)*, vol. 34, no. 2, pp. 292–302, Feb 2016.
- [98] Y. Fan, C. Xia, J. Chen, C. Y. Tsui, J. Jin, H. Shen, and B. Li, "A low-latency list successive-cancellation decoding implementation for polar codes," *IEEE Journal on Selected Areas in Comm. (JSAC)*, vol. 34, no. 2, pp. 303–317, Feb 2016.
- [99] G. Sarkis, P. Giard, A. Vardy, C. Thibault, and W. J. Gross, "Fast list decoders for polar codes," *IEEE Journal on Selected Areas in Comm (JSAC)*, vol. 34, no. 2, pp. 318–328, Feb 2016.
- [100] B. Y. Kong, H. Yoo, and I. C. Park, "Efficient sorting architecture for successive-cancellation-list decoding of polar codes," *IEEE Trans. on Circuits and Systems II: Express Briefs*, vol. 63, no. 7, pp. 673–677, July 2016.
- [101] J. Lin, C. Xiong, and Z. Yan, "A high throughput list decoder architecture for polar codes," *IEEE Trans. on Very Large Scale Integration (VLSI) Systems*, vol. 24, no. 6, pp. 2378–2391, June 2016.
- [102] C. Xiong, J. Lin, and Z. Yan, "Symbol-decision successive cancellation list decoder for polar codes," *IEEE Trans. on Signal Processing*, vol. 64, no. 3, pp. 675–687, Feb 2016.
- [103] M. B. Parizi, "Private communications," 2016.
- [104] R. Nasser, "Erasure schemes using generalized polar codes: Zero-undetected-error capacity and performance trade-offs," in *IEEE Int. Symp. on Inf. Theory (ISIT)*, July 2016, pp. 820–824.
- [105] M. Alsan and E. Telatar, "Polarization as a novel architecture to boost the classical mismatched capacity of b-dmcs," in *Information Theory Workshop (ITW), 2014 IEEE*, Nov 2014, pp. 366–370.